

**CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT**



Comments

**on
Review of the Telecom Commercial Communications Customer
Preference Regulations, 2018**

Introduction :

The Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018, brought significant improvements in managing unsolicited commercial communications (UCC). However, several challenges persist, particularly in enforcement, monitoring compliance, and keeping pace with the evolving nature of UCC. These challenges include:

1. Enforcement Challenges

- **Widespread Non-compliance:** Despite regulations, many telemarketers and businesses either fail to comply with customer preferences or exploit loopholes in the system. Some entities continue to send promotional communications without explicit consent, making enforcement difficult.

- **Limited Capacity for Penalty Collection:** Imposing penalties on violators is challenging, especially for small or unregistered telemarketers. TRAI's ability to enforce fines and ensure compliance from a large, decentralized market of telemarketers is limited.
- **Jurisdictional Issues:** Enforcement becomes even more complex when UCC is generated from outside India or from unregistered entities, making it difficult to trace the origin and enforce regulations across borders.

2. Monitoring Compliance

- **High Volume of Communications:** With the explosion of digital marketing and promotional activities, monitoring the sheer volume of calls and messages is a major hurdle. Tracking compliance in real-time for millions of daily communications is resource-intensive and technologically demanding.
- **Identifying Violators:** While blockchain technology has been introduced to track commercial communications, identifying violators remains challenging. Many offenders use multiple or unregistered numbers to bypass the system, making it difficult to trace and monitor repeat offenders.
- **Spoofing and Masking:** Telemarketers and spammers often use call spoofing (masking the original number) to hide their identity, which complicates the monitoring process. It allows them to bypass regulations without being detected.

3. Consumer Awareness and Participation

- **Lack of Consumer Participation:** Many consumers are either unaware of the option to register for Do Not Disturb (DND) services or

find the process cumbersome. This results in a lower-than-expected rate of registration, limiting the effectiveness of the preference management system.

- **Difficulty in Reporting Violations:** Even when consumers do receive unsolicited communications, the process of reporting violations is often seen as tedious or ineffective. Consumers may hesitate to file complaints, reducing the feedback necessary for effective monitoring and enforcement.

4. Evolving Nature of UCC

- **New Communication Channels:** As businesses adopt new channels such as social media, messaging apps (like WhatsApp and Telegram), and AI-driven chatbots, unsolicited communications are expanding beyond traditional SMS and calls. The current regulations may not fully cover these emerging platforms, leading to gaps in regulatory coverage.
- **Cross-channel Marketing:** Businesses are increasingly using integrated marketing strategies that combine SMS, emails, social media, and app notifications, blurring the lines between legitimate and unsolicited communication. This makes it harder to monitor and regulate communications across multiple platforms.
- **Personalized Advertising and Data Privacy:** With the rise of personalized advertising based on user data, there is a fine line between relevant marketing and intrusive UCC. Ensuring that businesses respect consumer data privacy while using targeted marketing is an evolving challenge.

5. Technological Advancements by Offenders

- **Automation and Bots:** Telemarketers are increasingly using automated systems, robocalls, and AI-driven bots to send out massive volumes of promotional content. These technologies allow them to operate at scale while avoiding detection, making it difficult for regulators to monitor and control UCC effectively.
- **Dynamic and Temporary Numbers:** Some marketers use dynamic numbers that change frequently, or temporary numbers, to evade detection by regulators and consumers. This makes it challenging to establish a pattern of abuse or track violators.

6. Coordination Between Stakeholders

- **Telecom Service Provider (TSP) Role:** Telecom service providers (TSPs) play a crucial role in managing UCC compliance, but their enforcement varies. Inconsistent implementation of regulations across TSPs weakens the system's overall effectiveness.
- **Inter-agency Coordination:** Effective monitoring and enforcement of UCC regulations require close cooperation between TRAI, telecom providers, consumer protection bodies, and law enforcement agencies. However, there are often gaps in coordination, leading to inefficiencies in tracking and penalizing offenders.

7. Global and Cross-border UCC

- **International Telemarketing:** Many unsolicited calls and messages originate from international numbers, especially from regions where Indian regulations don't apply. This makes it difficult to regulate or penalize foreign marketers who are not under TRAI's jurisdiction.

- **Lack of Global Standards:** The absence of unified global standards for regulating UCC makes it challenging to address cross-border communication issues effectively.

In short, the challenges in enforcing and monitoring TCCCPR 2018 regulations are compounded by the evolving nature of UCC, driven by technological advancements and new communication channels. Overcoming these hurdles requires a multi-faceted approach, including stronger enforcement mechanisms, more advanced monitoring technologies, better consumer participation, and greater coordination among stakeholders. The framework must also adapt to new platforms and forms of communication to stay relevant and effective in the face of changing marketing strategies.

Comments :

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.

Comments :

To better prevent promotional content and align with the service category templates as prescribed by TCCCPR 2018, the new definition of messages and calls could be as follows:

1. Messages:

○ **Transactional Messages:**

- **Definition:** Non-promotional, service-oriented messages that provide essential information regarding a transaction

or service requested by the customer. These messages should be strictly informational and include details such as one-time passwords (OTPs), transaction alerts, or order confirmations. **These messages must not contain any marketing or promotional content.**

- **Purpose:** To ensure the secure and efficient delivery of services without introducing promotional material that could be misconstrued as necessary communication.

- **Service (Informational) Messages:**

- **Definition:** Messages related to the ongoing use of a service or subscription by the customer. These messages should only offer necessary updates, reminders, or alerts regarding the service, without containing any promotional offers, advertisements, or marketing pitches. **Strictly no cross-selling or up-selling content should be permitted.**
- **Purpose:** To maintain clear and relevant communication with the customer regarding their current services, while strictly avoiding promotional content.

- **Promotional Messages:**

- **Definition:** Any message that is intended to advertise, promote, or market a product, service, or brand. Such messages should be sent only to recipients who have explicitly opted in to receive promotional content. **Promotional messages must be clearly marked as such, using designated sender IDs, and must allow for easy opt-out options.**

- **Purpose:** To ensure transparency and customer control over the receipt of promotional content, reducing the incidence of unsolicited promotional messages.

2. Calls:

○ **Transactional Calls:**

- **Definition:** Calls made solely for the purpose of completing a transaction or providing important service-related information to the customer. **No marketing, promotional offers, or advertisements should be allowed during these calls.**
- **Purpose:** To facilitate necessary communication regarding transactions or services, free from any promotional intent.

○ **Service (Informational) Calls:**

- **Definition:** Calls intended to provide important updates or information related to a service the customer is currently using. **These calls must remain strictly informational and are prohibited from including any promotional content.**
- **Purpose:** To keep customers informed about their services without subjecting them to unwanted promotional content.

Important Transactional Services :

Transactional services refer to essential and non-promotional communications that are directly related to a specific transaction or service initiated by the customer. These services ensure that important information

is delivered promptly and securely, without any marketing or promotional intent. Some of the most important transactional services include:

1. **Banking and Financial Services:**

- **OTP (One-Time Password) Messages:** Used for secure transactions, such as online banking, payment authorizations, and login verifications.
- **Transaction Alerts:** Notifications for account debits, credits, balance updates, and suspicious activity alerts.
- **Payment Confirmations:** Confirmation messages for completed transactions, such as bill payments, fund transfers, and e-commerce purchases.

2. **E-commerce and Online Shopping:**

- **Order Confirmations:** Messages confirming the receipt of an order and providing details such as order number, items purchased, and delivery timelines.
- **Shipping and Delivery Updates:** Notifications regarding the status of an order, including shipping confirmation, expected delivery date, and delivery confirmation.
- **Return and Refund Notifications:** Updates on the status of return requests, refunds processed, and any issues related to returns.

3. **Healthcare Services:**

- **Appointment Reminders:** Notifications about upcoming medical appointments, including date, time, and location.
- **Prescription Reminders:** Alerts for medication refills, prescriptions ready for pick-up, or follow-up instructions from healthcare providers.

- **Test Results and Medical Reports:** Secure delivery of lab test results or medical reports directly to the patient.

4. Telecommunication Services:

- **Bill Payment Reminders:** Notifications about upcoming or due payments for telecom services, including mobile, internet, and cable subscriptions.
- **Service Activation and Deactivation:** Confirmation messages related to the activation or deactivation of telecom services, such as roaming, data packs, or new connections.
- **Usage Alerts:** Alerts about data usage, call minutes, or SMS limits approaching exhaustion, and notifications about plan renewals.

5. Travel and Transportation Services:

- **Booking Confirmations:** Confirmation messages for flights, trains, buses, or hotel reservations, including booking reference numbers and travel details.
- **Check-in Reminders:** Notifications about the availability of online check-in for flights or reminders to check-in for accommodations.
- **Schedule Changes:** Alerts regarding changes in travel schedules, such as flight delays, cancellations, or rescheduled bookings.

6. Utilities and Government Services:

- **Bill Payment Confirmations:** Notifications confirming the payment of utility bills, such as electricity, water, gas, and property taxes.
- **Service Disruptions:** Alerts about scheduled maintenance, outages, or disruptions in utility services.

- **Government Notifications:** Important communications from government agencies, such as tax filing reminders, subsidy disbursements, or updates on government schemes.

7. Education Services:

- **Admission and Enrolment Updates:** Notifications about the status of applications, admissions, or enrollment in educational institutions.
- **Exam and Results Announcements:** Messages providing details about examination dates, results, and related announcements.
- **Fee Payment Reminders:** Reminders for due payments related to tuition fees, exam fees, or other educational expenses.

Purpose of Transactional Services:

These transactional services are vital for maintaining secure, transparent, and efficient communication between service providers and customers. They help in building trust by ensuring that critical information is delivered in a timely manner, **free from any promotional content that could distract or confuse the recipient.**

- **Promotional Calls:**
 - **Definition:** Calls with the specific purpose of promoting products, services, or brands. These calls are permitted only to customers who have opted in to receive such communications and must use designated caller IDs that clearly indicate the promotional nature of the call. **Customers must have the option to easily opt out of future promotional calls.**

- **Purpose:** To regulate promotional communications and ensure that only interested customers receive them, thus reducing the likelihood of unwanted promotional calls.

Purpose of New Definitions:

These new definitions aim to clearly delineate between different types of communications, ensuring that promotional content is only delivered to customers who have explicitly consented to receive it. By refining the definitions and strictly categorizing messages and calls, the new approach under TCCPR 2018 seeks to enhance customer protection against unsolicited promotional content while maintaining necessary service-related communication.

Misuse of Service Explicit Templates of offline consent :

To prevent the misuse of Service Explicit Templates for pushing promotional content under the guise of offline consent, thorough reviews are essential. Here are the key types of reviews that should be implemented:

1. Content Review:

- **Purpose Verification:** Ensure that the content of the message strictly adheres to the purpose of the service or transaction for which the template is approved. It should not contain any promotional elements.
- **Language Check:** The language used should be neutral, avoiding any phrases that could be construed as promotional or suggestive of further engagement beyond the service explicitly requested.

- **Scope Limitation:** Verify that the message content does not exceed the scope of the service or transaction. Any content that deviates into promotional territory should be flagged.

2. Consent Verification:

- **Offline Consent Documentation:** Ensure that any claimed offline consent is properly documented and auditable. The documentation should clearly specify that the customer has agreed to receive service-related messages and not promotional content.
- **Consent Validity:** Regularly check the validity of the consent, ensuring it has not expired or been revoked.

3. Template Review:

- **Periodic Audits:** Conduct regular audits of all active service explicit templates to ensure they continue to comply with regulatory guidelines. Templates should be reviewed periodically for any changes or drift towards promotional content.
- **Approval Process:** Implement a robust approval process where new templates or changes to existing ones undergo a rigorous review by a compliance team before they can be used.

4. Usage Monitoring:

- **Message Tracking:** Monitor the usage of approved templates to ensure they are being used exclusively for the stated purpose. Any deviations or patterns of misuse should be flagged for further investigation.

- **Complaint Analysis:** Analyze complaints from recipients to identify any trends of misuse, indicating that promotional content is being sent under the guise of service messages.

5. Compliance Audits:

- **Third-Party Audits:** Engage third-party auditors to periodically review the implementation of these guidelines, ensuring that the processes are robust and free from potential conflicts of interest.
- **Internal Reviews:** Regular internal reviews by the compliance and legal teams to ensure adherence to both the letter and the spirit of the regulations.

These types of reviews will help maintain the integrity of Service Explicit Templates and prevent their misuse for promotional content, thereby protecting consumer rights.

Different Regulation for Voice Calls :

The regulation of commercial voice calls and text messages should be differ due to their distinct characteristics, uses, and impacts on consumers. Here are some considerations for why the regulation should be different:

1. Intrusiveness and User Experience

- **Voice Calls:** Voice calls are generally more intrusive than text messages. They demand immediate attention and can disrupt the user more significantly, especially if they occur at inconvenient times.
- **Text Messages:** Text messages, while potentially annoying, are less disruptive. They can be read and responded to at the user's convenience.

2. Content Delivery and Context

- **Voice Calls:** The content of voice calls is delivered in real-time, which might not allow the user to process or review the information as thoroughly as a text message. This can be particularly concerning for promotional or scam-related calls.
- **Text Messages:** Text messages provide a record that can be reviewed, ignored, or reported later. This allows for more control and reference for the user.

3. Privacy and Consent

- **Voice Calls:** Users may be more sensitive to privacy concerns related to voice calls, particularly if they feel pressured during the interaction. Regulations may need to ensure stricter consent mechanisms for voice calls.
- **Text Messages:** While privacy is also a concern for text messages, the lower level of intrusion might justify a different level of regulation, particularly around opt-in and opt-out mechanisms.

4. Technical Differences

- **Voice Calls:** The technology behind voice calls, including the possibility of spoofing or robocalling, might require different technical safeguards and regulatory approaches.
- **Text Messages:** The regulation of text messages might focus more on filtering mechanisms, content categorization, and delivery methods, such as short codes.

5. Consumer Protection

- **Voice Calls:** Given the potential for greater consumer harm through voice calls, such as scams or high-pressure sales tactics, stricter regulations might be necessary.
- **Text Messages:** While still a potential avenue for scams, text messages might be seen as less risky, possibly requiring a different regulatory framework focusing on spam prevention.

6. Market Practices

- **Voice Calls:** The commercial use of voice calls often involves direct interaction, which might require regulations to address specific practices such as call recording, caller identification, and do-not-call lists.
- **Text Messages:** Regulations for text messages might focus more on content compliance, frequency of messages, and user consent for receiving promotional content.

In summary, the regulation of commercial voice calls and text messages could justifiably differ due to the varying degrees of intrusiveness, privacy concerns, consumer protection needs, and technical characteristics. A tailored approach could help balance the interests of consumers and businesses more effectively.

Mechanism to check the veracity of call contents :

Ensuring the veracity of call contents, especially in a commercial context, is critical for protecting consumers from fraud, misinformation, and other unethical practices. A foolproof mechanism would likely involve a combination of technological, regulatory, and procedural measures. Here's a comprehensive approach:

1. Caller ID Authentication and Verification

- **STIR/SHAKEN Protocol:** Implement the STIR (Secure Telephone Identity Revisited) and SHAKEN (Signature-based Handling of Asserted Information Using toKENs) framework, which helps authenticate the origin of calls and ensures that the Caller ID information is accurate. This reduces the chances of spoofed calls.
- **Verified Caller IDs:** Require businesses to register and verify their Caller IDs with telecom operators, ensuring that the caller information presented to the recipient is trustworthy.

2. Recording and Archiving Calls

- **Mandatory Call Recording:** For certain types of commercial calls (e.g., telemarketing, customer service, financial services), require that all calls be recorded and stored securely for a specified period.
- **Access to Recordings:** Provide consumers with access to these recordings upon request, particularly in cases of disputes or complaints. This ensures transparency and accountability.

3. Voice Analytics and AI Monitoring

- **Real-time Voice Analysis:** Use AI-based voice analytics to monitor calls in real-time for signs of fraudulent activity, misrepresentation, or aggressive sales tactics. These systems can flag suspicious calls for further review.
- **Post-Call Analysis:** Implement AI tools that analyze recorded calls for compliance with regulatory standards, truthfulness, and consistency of information. These tools can detect anomalies or patterns indicative of fraud.

4. Regulatory Oversight and Compliance

- **Regular Audits:** Establish regular audits of companies that engage in large volumes of commercial calls. Audits should include reviewing call scripts, recordings, and consumer feedback.
- **Compliance Certification:** Require companies to obtain and maintain a compliance certification for their call practices. Non-compliance should lead to penalties, including revocation of the certification.

5. Consumer Feedback and Reporting

- **Feedback Mechanism:** Implement an easy-to-use system for consumers to provide feedback or report suspicious calls. This can be integrated into mobile apps, where users can flag a call as suspicious or provide details about misleading content.
- **CAG's and Whistleblower Protections:** Encourage internal reporting by providing protections and incentives for employees who report unethical call practices within their organizations.

6. Content Standardization and Scripting

- **Approved Call Scripts:** Require businesses to use pre-approved scripts for commercial calls, particularly in sensitive areas like financial services or healthcare. Scripts should be designed to ensure clarity, transparency, and accuracy of information.
- **Dynamic Script Monitoring:** Use technology to monitor deviations from the approved script during live calls. Significant deviations could trigger real-time alerts or reviews.

7. Consumer Education

- **Awareness Campaigns:** Conduct regular consumer education campaigns about recognizing and reporting fraudulent or misleading calls. Educated consumers are more likely to detect and report suspicious activities.
- **Guidelines on Interaction:** Provide consumers with guidelines on how to interact with commercial calls, such as asking for written confirmation of any offers or deals discussed over the phone.

8. Data and Identity Verification

- **Two-Factor Authentication (2FA):** For high-risk transactions or sensitive information sharing, require two-factor authentication during the call to verify the identity of both the caller and the recipient.
- **Data Verification Services:** Use third-party services to verify the data being communicated in real-time, ensuring that any claims made during the call are accurate and verifiable.

9. Legal and Regulatory Framework

- **Legal Consequences for Misrepresentation:** Strengthen legal frameworks to impose significant penalties for businesses that engage in fraudulent or misleading practices during calls.
- **Consumer Protection Laws:** Enforce robust consumer protection laws that give consumers recourse if they are misled or harmed by false information provided during a call.

10. Transparency and Disclosure Requirements

- **Mandatory Disclosures:** Require that certain disclosures be made at the beginning and end of commercial calls, such as the purpose of the call, the identity of the caller, and the recording status.

- **Post-Call Summary:** Provide consumers with a summary of the call content via text or email, especially for transactions or agreements made during the call. This summary should include all key points discussed and any commitments made.

By integrating these measures, the veracity of call contents can be effectively checked and maintained, significantly reducing the potential for fraud, misrepresentation, and consumer harm.

In Different Countries :

The regulation of commercial calls and text messages varies widely by country, with some countries implementing different regulatory frameworks for these two forms of communication due to their distinct characteristics. Below are examples of countries where regulations for commercial calls differ from those for text messages:

1. United States

- **Calls:** The Telephone Consumer Protection Act (TCPA) regulates commercial calls, including robocalls, telemarketing, and other unsolicited calls. The TCPA requires prior express written consent for most telemarketing calls, and violations can result in substantial fines.
- **Text Messages:** While also covered under the TCPA, text messages are treated slightly differently. Text messaging campaigns require opt-in consent from recipients, but the regulations are generally more permissive than those for calls. The CAN-SPAM Act also regulates commercial texts, focusing on preventing misleading content.

2. United Kingdom

- **Calls:** The Privacy and Electronic Communications Regulations (PECR) govern commercial calls. Businesses must have prior consent to make unsolicited marketing calls, and there are strict rules against calling numbers registered with the Telephone Preference Service (TPS).
- **Text Messages:** Text messages are also regulated under PECR, but the rules are more focused on consent and transparency rather than the act of sending the message itself. Businesses must obtain consent before sending marketing texts, but enforcement and penalties differ from those for calls.

3. Canada

- **Calls:** The Canadian Radio-television and Telecommunications Commission (CRTC) enforces regulations under the Telecommunications Act and Canada's Anti-Spam Legislation (CASL). Commercial calls are tightly regulated, with requirements for consent and the ability to register on the National Do Not Call List (DNCL).
- **Text Messages:** CASL also covers text messages, but the focus is more on ensuring consent and providing clear unsubscribe mechanisms. The regulation of text messages tends to be less stringent compared to voice calls, particularly in terms of enforcement.

4. Australia

- **Calls:** The Do Not Call Register Act 2006 and the Spam Act 2003 regulate commercial calls. Telemarketers must respect the Do Not

Call Register and can only contact individuals who have not opted out of receiving such calls.

- **Text Messages:** The Spam Act 2003 also covers commercial text messages, requiring businesses to obtain consent before sending marketing texts and to include an opt-out mechanism. However, enforcement practices and consumer protections differ, with calls being more heavily regulated due to their intrusive nature.

6. European Union

- **Calls:** In the EU, the General Data Protection Regulation (GDPR) and the ePrivacy Directive set out rules for commercial calls, requiring explicit consent and giving consumers the right to object to marketing calls.
- **Text Messages:** Text messages are also regulated under GDPR and ePrivacy, but the rules often focus on data protection and privacy, with a stronger emphasis on consent for data processing. The distinction in enforcement practices means that calls often receive closer scrutiny due to their potential for greater consumer disruption.

7. Singapore

- **Calls:** The Personal Data Protection Act (PDPA) includes specific provisions for the Do Not Call (DNC) Registry, which regulates commercial calls. Organizations must check the DNC Registry before making marketing calls, and there are penalties for non-compliance.
- **Text Messages:** The PDPA also regulates text messages, but the approach is more focused on ensuring clear opt-out options and transparency in marketing communications. The penalties for

violations in text messaging are typically less severe than for unsolicited calls.

These examples illustrate that while both commercial calls and text messages are subject to regulation, the frameworks often differ in how they treat these two forms of communication, reflecting their unique impacts on consumers.

We are agreeing with the categorization of commercial messages prepared by TRAI. **We can add Service or Utility messages.**

Regulating the use of Auto Dialler or Robbo-call :

Negative impact on consumers of auto dialer promotional calls :

Auto-dialler promotional calls, often used for marketing and telemarketing purposes, can have several negative impacts on consumers. These unsolicited and sometimes intrusive calls are affecting consumers in various ways:

Negative Impacts on Consumers:

1. Invasion of Privacy:

- **Unsolicited Calls:** Auto-dialler promotional calls often invade personal privacy by reaching consumers without their explicit consent. These calls interrupting in personal time, work, or other important activities, leading to frustration and a sense of intrusion.
- **Frequency and Timing:** The high frequency of these calls, often at inconvenient times (early mornings, late evenings, or

weekends), is particularly bothersome, causing significant annoyance.

2. Emotional and Psychological Stress:

- **Constant Interruptions:** Frequent interruptions from auto-dialler calls leads to stress and anxiety, especially when they occur repeatedly throughout the day.
- **Aggressive Marketing:** Some auto-dialler calls employ aggressive marketing tactics, which is overwhelming and cause discomfort or pressure, particularly for vulnerable consumers.

3. Financial Costs:

- **Unintended Charges:** In some cases, consumers might unintentionally incur charges, especially when calls are made to mobile numbers with limited plans or international roaming.
- **Opportunity Cost:** Time spent dealing with these calls is also be seen as a financial loss, as it takes away from more productive or meaningful activities.

4. Scams and Fraud Risks:

- **Increased Risk of Scams:** Auto-dialler calls sometimes be used as a tool for scams, where fraudulent entities pose as legitimate businesses to extract personal or financial information from unsuspecting consumers.
- **Misleading Information:** Consumers are misled by promotional offers that seem too good to be true, leading to financial losses or signing up for services/products they don't need.

5. Impact on Vulnerable Groups:

- **Elderly and Technologically Unsavvy:** Elderly consumers or those who are less familiar with technology may be particularly

vulnerable to the pressure and confusion caused by these calls, potentially leading to unwise financial decisions or scams.

- **Low-Income Consumers:** Individuals from low-income backgrounds feel pressured by persistent calls to make purchases or sign up for services they cannot afford, leading to financial strain.

6. Reduction in Trust:

- **Distrust in Legitimate Communications:** Constant promotional calls is eroding consumer trust in legitimate communications from businesses. Consumers starts ignoring important calls, fearing they are just more unsolicited promotions.
- **Negative Perception of Brands:** Repeated, unwanted calls lead to a negative perception of the brand or company, damaging its reputation and relationship with the consumer.

7. Disruption of Essential Services:

- **Missed Important Calls:** Auto-dialler calls causes consumers to miss or ignore important calls, including those related to health, work, or personal emergencies, due to the saturation of unwanted calls.

8. Legal and Regulatory Challenges:

- **Non-Compliance Issues:** Some auto-dialler calls are not complied with regulations such as the National Do Not Call Registry, leading to legal disputes and additional stress for consumers who believed they had opted out of such communications.
- **Difficulty in Opting Out:** Many consumers find it challenging to opt out of these calls, either because the process is

cumbersome or because companies do not honour opt-out requests, leading to ongoing frustration.

In short Auto-dialler promotional calls, while useful for businesses to reach a large audience quickly, is having significant negative impacts on consumers. These include privacy invasion, emotional stress, financial burdens, increased vulnerability to scams, and a general decline in the quality of life. For these reasons, stricter regulations, better enforcement, and more consumer-friendly opt-out mechanisms are often advocated to mitigate these adverse effects.

Rules and Regulations :

We are in agreement with the possible measures prescribed by the TRAI. Our suggestions are as follows :

To effectively regulate the use of autodialers and robocalls for commercial communications, strict rules and regulations should be implemented to protect consumers from unwanted and potentially harmful practices. Here are key measures that should be considered:

1. Explicit Consent Requirement:

- **Prior Written Consent:** Businesses must obtain explicit, written consent from consumers before sending robocalls or using autodialers for commercial purposes. This consent should clearly outline the types of communications the consumer is agreeing to receive.
- **Clear Opt-In Process:** Consent should be obtained through a clear opt-in process, ensuring that consumers fully understand what they are signing up for.

2. Strict Identification Rules:

- **Caller Identification:** Every robocall must clearly identify the caller, including the name of the business, the purpose of the call, and a valid phone number or contact information.
- **Automated Disclosure:** The robocall must begin with a brief disclosure identifying it as an automated call and providing information on how to opt out.

3. Opt-Out Mechanism:

- **Immediate Opt-Out:** Robocalls should provide an immediate and easy option for consumers to opt out of future calls, such as pressing a specific key.
- **Compliance with Opt-Out Requests:** Businesses must honour opt-out requests promptly and must not contact the consumer again once they have opted out.

4. Time Restrictions:

- **Call Timing:** Autodialers and robocalls should only be permitted during certain hours, typically between 9:00 AM and 9:00 PM local time, to avoid disturbing consumers at inappropriate times.
- **Frequency Limits:** Limit the number of robocalls that can be made to a single consumer in a specified time period to prevent harassment.

5. Penalties for Non-Compliance:

- **Significant Fines:** Implement substantial fines for violations of these rules to deter non-compliance. Penalties should be severe enough to discourage businesses from engaging in unethical practices.

- **Legal Recourse:** Provide consumers with legal recourse, including the ability to sue businesses for unauthorized robocalls, with provisions for statutory damages.

6. Monitoring and Reporting:

- **Robust Monitoring System:** Establish a system for monitoring robocall activity and ensuring compliance with regulations. This could involve regular audits and assessments.
- **Consumer Reporting Mechanism:** Create an easy and accessible way for consumers to report unwanted robocalls, including a dedicated helpline or online portal.

7. Exemptions and Special Cases:

- **Public Safety and Emergency Communications:** Exemptions should be made for robocalls related to public safety, emergencies, and other essential services, but these should be clearly defined to avoid misuse.
- **Non-Commercial Calls:** Differentiate between commercial robocalls and those from charities, political campaigns, or surveys, applying specific rules to each category.

8. Technological Safeguards:

- **Anti-Spoofing Technology:** Require the use of technology that prevents caller ID spoofing, which is often used to mask the true identity of the caller.
- **Call Authentication:** Implement call authentication protocols, such as STIR/SHAKEN, to verify the legitimacy of robocalls and prevent fraudulent activities.

9. Transparency and Record-Keeping:

- **Record of Consent:** Businesses should be required to maintain records of consumer consent, including the date, time, and method of consent.
- **Disclosure of Data Use:** Businesses must disclose how consumer data, including phone numbers, is being used, stored, and shared.

These regulations can help balance the legitimate use of Auto Dialers and robocalls for commercial purposes with the need to protect consumer privacy and prevent abuse.

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.

Comments : **Yes. Mentioned Above.**

Yes, **explicit consent** should be made mandatory for receiving promotional communications through autodialers or robocalls. This requirement serves as a crucial consumer protection measure to ensure that individuals have control over the communications they receive and are not subjected to unsolicited or unwanted promotional messages. Here's why mandatory explicit consent is important:

1. Consumer Autonomy and Privacy:

- **Informed Choice:** By requiring explicit consent, consumers are given the power to choose whether or not they wish to receive promotional

communications. This protects their autonomy and ensures they are not bombarded with unwanted calls.

- **Protection of Personal Data:** Consent requirements help safeguard personal information, ensuring that businesses cannot misuse phone numbers without permission.

2. Prevention of Spam and Unwanted Communications:

- **Reducing Intrusiveness:** Autodialers and robocalls can be intrusive, especially if they occur frequently or at inconvenient times. Mandatory consent helps reduce the volume of such calls, limiting them to those who have explicitly agreed to receive them.
- **Minimizing Annoyance:** Unsolicited promotional calls can be annoying and disruptive. Explicit consent ensures that only interested consumers are contacted, improving the overall consumer experience.

3. Legal Compliance and Consumer Protection Laws:

- **Alignment with Regulatory Standards:** Many consumer protection laws and regulations, such as the Telephone Consumer Protection Act (TCPA) in the United States, already require explicit consent for certain types of robocalls. Making consent mandatory aligns with these legal standards.
- **Avoiding Legal Penalties:** Businesses that fail to obtain explicit consent may face significant legal penalties, including fines and lawsuits, which can be costly and damaging to their reputation.

4. Building Trust with Consumers:

- **Enhancing Brand Reputation:** When businesses respect consumer preferences and seek explicit consent, they build trust and credibility with their audience. This can lead to better customer relationships and higher engagement rates.
- **Positive Consumer Perception:** Consumers are more likely to have a positive perception of brands that respect their communication preferences, leading to increased loyalty and long-term customer retention.

5. Ethical Business Practices:

- **Respecting Consumer Rights:** Mandatory consent reflects ethical business practices by prioritizing the rights and preferences of consumers over aggressive marketing tactics.
- **Encouraging Responsible Marketing:** Requiring explicit consent promotes responsible marketing, where businesses target only those who have shown interest in their products or services.

6. Clear Record-Keeping and Accountability:

- **Documenting Consent:** Mandatory explicit consent requires businesses to keep clear records of when and how consent was obtained. This documentation can serve as proof of compliance in case of disputes.
- **Accountability:** With a consent-based approach, businesses are held accountable for their marketing practices, ensuring they adhere to legal and ethical standards.

In summary, making explicit consent mandatory for promotional communications via autodialers or robocalls is essential for protecting

consumer rights, reducing unwanted communications, and fostering responsible marketing practices. It ensures that consumers are only contacted by businesses they have explicitly chosen to engage with, leading to a more respectful and effective communication environment.

Other Possible Measures :

To curb the use of autodialers or robocalls without the consent of recipients, several additional measures can be implemented beyond mandatory explicit consent. These measures can help reduce the frequency and impact of unsolicited robocalls and enhance consumer protection. Here are some key strategies:

1. Strengthening Penalties and Enforcement:

- **Increased Fines and Penalties:** Implement harsher penalties for businesses that violate robocall regulations, including significant fines per unauthorized call. These penalties should be sufficient to deter non-compliance.
- **Enhanced Enforcement:** Increase the resources and TRAI to enforce robocall laws effectively. This includes conducting investigations, imposing penalties, and shutting down repeat offenders.

2. Mandatory Caller ID Authentication:

- **STIR/SHAKEN Protocols:** Require the implementation of STIR/SHAKEN protocols, which verify the authenticity of caller ID information. This technology helps prevent spoofing, where callers falsify their caller ID to appear legitimate.

- **Caller ID Transparency:** Mandate that all robocalls include accurate and transparent caller ID information, including the name of the business and a valid contact number.

3. Establishing National and Regional Do-Not-Call (DNC) Registries:

- **Easy Opt-Out:** Strengthen and promote Do-Not-Call registries where consumers can easily register their phone numbers to avoid receiving unsolicited robocalls.
- **Strict Compliance Monitoring:** Implement strict monitoring to ensure that businesses comply with DNC registries and do not contact registered numbers. Violators should face significant penalties.

4. Technological Solutions for Consumers:

- **Call-Blocking Services:** Encourage or mandate telecom providers to offer call-blocking services that allow consumers to block suspected robocalls. These services can use algorithms to identify and block likely robocalls.
- **Robocall Mitigation Apps:** Promote the use of robocall mitigation apps that screen and block unwanted calls. Some apps allow users to report and block numbers associated with robocalls.

5. Public Awareness Campaigns:

- **Consumer Education:** Launch public awareness campaigns to educate consumers about their rights regarding robocalls, how to report violations, and how to use available tools to block unwanted calls.

- **Highlight Reporting Channels:** Make consumers aware of easy ways to report illegal robocalls, such as through a dedicated helpline, website, or app.

6. Network-Level Interventions:

- **Carrier-Level Blocking:** Require telecom carriers to implement network-level interventions that automatically block or flag suspicious robocalls before they reach consumers.
- **Traffic Monitoring:** Encourage carriers to monitor traffic patterns to identify and block robocall operations, especially those originating from known bad actors.

7. Third-Party Certification and Auditing:

- **Certification Programs:** Establish certification programs for businesses that use robocalls, ensuring they adhere to best practices and legal requirements. Certified businesses can be audited periodically to ensure ongoing compliance.
- **Third-Party Audits:** Require businesses that use autodialers to undergo regular third-party audits to ensure they are following consent requirements and other regulations.

8. Regulation of Call Origination Points:

- **Licensing and Oversight:** Introduce regulations that require call centers and businesses using autodialers to obtain licenses. These licenses can be revoked in case of non-compliance with robocall laws.

- **International Collaboration:** Work with international partners to regulate and block robocalls originating from overseas, particularly in countries where regulation may be weaker.

9. Limiting the Use of Automatic Dialing Systems:

- **Usage Caps:** Impose limits on the number of calls that can be made by autodialers within a certain timeframe, especially to numbers not on a pre-approved list.
- **Pre-Dialling Checks:** Require that autodialers perform checks to ensure numbers have provided consent before initiating calls.

10. Legal Recourse for Consumers:

- **Class-Action Lawsuits:** Empower consumers to file class-action lawsuits against businesses that violate robocall regulations, making it easier for individuals to seek compensation.
- **Statutory Damages:** Allow consumers to claim statutory damages for each unsolicited robocall received without consent, providing a strong deterrent against violations.

11. Data Protection and Privacy Regulations:

- **Stricter Data Handling Rules:** Implement regulations that restrict how businesses collect, store, and use phone numbers for marketing purposes. Data breaches and misuse should lead to severe penalties.
- **Prohibition of Data Sharing Without Consent:** Prohibit the sharing or selling of phone numbers and other personal data without explicit consent from the consumer.

12. Whitelisting of Trusted Callers:

- **Opt-In Whitelisting:** Create a system where consumers can opt-in to receive calls only from whitelisted, trusted callers, blocking all other calls automatically.
- **Priority Call Systems:** Develop systems that allow emergency or critical calls to bypass blocking, while promotional or non-essential calls are subject to stricter controls.

Implementing these measures can significantly reduce the number of unauthorized robocalls, ensuring that consumers are only contacted when they have given explicit permission, and making it more difficult for bad actors to exploit the system.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

- **Content Moderation:** While these rules primarily deal with digital media and social media platforms, they also impose certain responsibilities on intermediaries (including telecom operators) to prevent misuse of their platforms for spam or unauthorized communications.

These laws and regulations collectively aim to protect consumers from the nuisance and potential harm of unsolicited robocalls while providing a framework for businesses to conduct legitimate commercial communications responsibly.

The TRAI should be committed to doing what they can to protect the consumers from these unwelcome situations and should crack down on illegal calls in a variety of ways like :

- ✓ Spending on enforcement actions against illegal robocallers.

- ✓ Empowering phone companies to block by default illegal or unwanted calls based on reasonable call analytics before the calls reach consumers.
- ✓ Allowing consumer options on tools to block calls from any number that doesn't appear on a customer's contact list or other "white list."
- ✓ Requiring phone companies to implement caller ID authentication to help reduce illegal spoofing.
- ✓ Requiring gateway providers to shut down the on-ramps for international illegal robocall traffic.
- ✓ Making consumer complaint data available to enable better call blocking and labelling solutions.

There are several emerging technologies designed to combat robocalls more effectively:

STIR/SHAKEN Protocols: These protocols (Secure Telephony Identity Revisited/Signature-based Handling of Asserted Information Using toKENs) help verify the legitimacy of calls by ensuring that the caller ID information is accurate and not spoofed.

AI and Machine Learning: Advanced AI and machine learning algorithms are being used to detect and block robocalls. These systems analyze call patterns and behaviors to identify and filter out unwanted calls.

Caller ID Authentication: Technologies that provide better caller ID by applying a token to verified phone numbers or displaying a branded logo on the receiver's phone are being developed.

Robocall Blocking Apps: There are numerous apps available that use databases of known robocall numbers and employ algorithms to identify and block suspicious calls.

Regulatory Measures: Regulatory bodies like the FCC and FTC are implementing new rules and protections against AI-generated robocalls and other emerging technologies used in telemarketing fraud.

These technologies, combined with stricter regulations and consumer education, are making significant strides in reducing the prevalence of robocalls.

The challenges in implementing AI-based robocall detection :

Implementing AI-based robocall detection comes with several challenges, including:

1. **Evolving Robocall Tactics:** Robocallers constantly adapt their strategies to bypass detection systems. AI models must continuously evolve to keep up with new tactics like voice mimicry, spoofing legitimate numbers, and changing scripts.
2. **High Volume of Data:** The sheer volume of calls made daily makes it difficult to process and analyze data in real-time. AI systems need to be highly efficient to handle this large-scale data without slowing down the response time.
3. **False Positives and Negatives:** AI models might incorrectly classify legitimate calls as robocalls (false positives) or miss identifying actual robocalls (false negatives). Balancing precision and recall in the detection algorithms is challenging.
4. **Caller ID Spoofing:** Robocallers often use caller ID spoofing, where they manipulate the caller ID to display a trusted or local number. Detecting spoofed calls requires advanced techniques, as spoofing complicates identification.
5. **Data Privacy Concerns:** Implementing AI-based systems involves analyzing vast amounts of call data, which can raise privacy concerns.

Ensuring compliance with data protection regulations while maintaining system effectiveness is a significant challenge.

6. **Integration with Existing Systems:** Integrating AI-based detection with existing telecommunication infrastructure, especially across different carriers and jurisdictions, can be complex and may require standardization.
7. **Resource Intensity:** AI models, especially those that are sophisticated enough to detect nuanced robocall tactics, require significant computational resources and expertise to develop, deploy, and maintain.
8. **User Trust and Adoption:** Users might be sceptical about AI-based systems, especially if they experience false positives. Building trust in these systems is crucial for widespread adoption.
9. **Legal and Regulatory Challenges:** The legal landscape regarding robocall detection and prevention is complex, with varying regulations across regions. Compliance with these regulations while effectively deploying AI-based systems is challenging.
10. **Global Variations in Call Patterns:** Robocall patterns can vary significantly between different regions, making it difficult to develop a one-size-fits-all solution. AI models must be tailored to specific locales, requiring extensive localization efforts.

Addressing these challenges requires a combination of advanced technology, regulatory support, and collaboration among stakeholders in the telecommunications industry.

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.

Comments : **Mentioned above.**

To ensure that pre-recorded calls with predefined content comply with regulations and do not deliver unauthorized or promotional content to consumers, the following process can be followed:

1. Content Review and Approval

- **Pre-Screening:** The content of pre-recorded calls should be pre-screened and approved by a regulatory body or a designated compliance team within the organization. This step ensures that the content meets legal and regulatory standards, such as those outlined in the Telecom Commercial Communications Customer Preference Regulations (TCCCPR) 2018.
- **Template Registration:** All pre-recorded call content templates should be registered with the relevant authorities (e.g., TRAI in India). This registration ensures that only approved content is used in calls.

2. Scrubbing Process

- **Filtering Against DND Registry:** Before the call is delivered, scrub the content against the National Do Not Disturb (DND) registry to ensure that it is not sent to consumers who have opted out of receiving promotional messages or calls.
- **Content Scrubbing Tools:** Utilize automated content scrubbing tools that can analyze the pre-recorded message for any unapproved

language, phrases, or promotional material. These tools can flag or block content that does not match the approved template.

3. Verification and Testing

- **Sample Testing:** Regularly test a sample of pre-recorded calls to verify that the content aligns with the approved template. This can help identify any discrepancies or unauthorized changes to the content.
- **Third-Party Audits:** Consider periodic audits by an independent third party to ensure that the content of pre-recorded calls is being accurately scrubbed and delivered as per the regulatory guidelines.

4. Delivery Control

- **Call Tracking:** Implement call tracking mechanisms to monitor the delivery of pre-recorded calls. This tracking can include logging the content delivered, the recipient, and the time of the call.
- **Real-Time Monitoring:** For high-risk content, use real-time monitoring systems that can interrupt or block a call if it detects unauthorized content during the delivery process.

5. Consumer Feedback Mechanism

- **Reporting and Resolution:** Provide consumers with an easy way to report any unsolicited or non-compliant pre-recorded calls. Address these reports promptly and take corrective action if necessary.
- **Regular Updates:** Regularly update the scrubbing process to account for new regulations, consumer preferences, and technological advancements.

This process helps ensure that pre-recorded calls are compliant with regulations and respect consumer preferences, thus minimizing the risk of unauthorized or promotional content being delivered.

The process of scrubbing pre-recorded calls before delivery to consumers is a global practice with variations depending on the country's regulatory environment. However, the following common steps are generally followed worldwide to ensure that pre-recorded calls comply with local laws and regulations:

1. Content Registration and Approval

- **Regulatory Approval:** In many countries, such as the United States (under the TCPA), Europe (under GDPR), and Australia (under ACMA), pre-recorded call content must be approved by regulatory authorities or adhere to strict guidelines. Organizations may need to register their message templates with these authorities to ensure compliance.
- **Internal Compliance Checks:** Organizations often have internal compliance teams that review the content of pre-recorded messages to ensure they meet legal requirements and avoid any unauthorized promotional material.

2. Scrubbing Against Do-Not-Call Lists

- **National Do-Not-Call (DNC) Registries:** Most countries maintain a DNC registry, where consumers can opt out of receiving promotional calls. Before delivering pre-recorded calls, the content and recipient lists are scrubbed against these national registries to avoid violating consumer preferences.

- **International Scrubbing Services:** For global campaigns, international scrubbing services are used to cross-check consumer numbers against DNC lists from multiple countries.

3. Automated Content Scrubbing

- **Artificial Intelligence (AI) Tools:** Advanced AI tools are often employed to automatically scrub pre-recorded messages. These tools can detect and flag any content that does not conform to approved templates or includes unauthorized language, ensuring that only compliant messages are delivered.
- **Keyword Filtering:** Automated systems may also use keyword filtering to detect and block any content that includes unapproved promotional material or sensitive information that could breach regulations like GDPR.

4. Regular Audits and Testing

- **Routine Audits:** Companies often conduct regular audits of their pre-recorded call processes to ensure ongoing compliance. These audits may be conducted internally or by third-party auditors to identify any potential risks or breaches.
- **Sample Call Testing:** Sample calls are regularly tested to ensure that the content delivered matches the approved script and that no unauthorized content is being sent to consumers.

5. Real-Time Monitoring and Controls

- **Live Call Monitoring:** In some regions, real-time monitoring systems are used to oversee the delivery of pre-recorded calls. These systems

can automatically block or modify content if they detect a deviation from the approved script.

- **Call Tracking and Logs:** Detailed logs of pre-recorded calls are maintained, including the content delivered, the time of the call, and the recipient. This helps in post-call audits and resolving any complaints from consumers.

6. Consumer Opt-Out Mechanisms

- **Opt-Out Options:** Pre-recorded calls often include a mechanism for consumers to opt out of future calls, which is a requirement in many countries. This could be a button press during the call or a follow-up message that provides an opt-out link.
- **Compliance with Opt-Out Requests:** Compliance with consumer opt-out requests is closely monitored. Systems are updated promptly to ensure that no further calls are made to those who have opted out.

7. Global Regulatory Adaptation

- **Country-Specific Compliance:** For international businesses, scrubbing processes are adapted to comply with the specific regulations of each country. This might involve different content review processes, additional language filters, or varying levels of consumer consent required.
- **Cultural Sensitivity:** Content is also reviewed for cultural sensitivity and appropriateness in different regions, ensuring that the message resonates positively with the target audience.

Conclusion

While the specific processes may vary depending on local laws and regulations, the overarching approach to scrubbing pre-recorded call content remains consistent globally. The key steps include regulatory approval, DNC scrubbing, automated content checks, regular audits, real-time monitoring, and strict adherence to consumer preferences. This helps businesses deliver compliant and non-intrusive pre-recorded messages worldwide.

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.

Comments :

Revised Categorization of the Commercial Communication should be :

1. Transactional - T
2. Promotional - P
3. Government - G and
4. Service - S.

Attaching a prefix to the header for identifying the Access Provider and Service area can be useful for consumers in several ways:

1. **Transparency:** It allows consumers to easily identify the source of the communication, which enhances transparency. Knowing the Access Provider and Service area can help consumers trust the authenticity of the communication.

2. **Fraud Prevention:** This can be particularly useful in preventing fraud. Consumers can be more cautious if they receive a call or message from an unexpected Access Provider or Service area.
3. **Better Decision-Making:** Consumers can make more informed decisions regarding whether to answer a call, respond to a message, or take action based on the information provided.
4. **Service Quality Monitoring:** It helps consumers track the quality of service from specific providers and service areas, potentially guiding them in choosing a more reliable provider.
5. **Regulatory Compliance:** It ensures that the communication is in compliance with regulatory requirements, which can provide consumers with an additional layer of security.
6. **Accountability:** It holds service providers accountable for the messages sent through their network. If there are any issues or complaints, it becomes easier to trace the source.

Overall, such a prefix system can enhance consumer confidence and protect against unsolicited or fraudulent communications.

Challenges in Implementing such system :

Implementing a system where prefixes are attached to headers for identifying Access Providers and Service Areas comes with several challenges:

- **Technical Integration:** Integrating this system across various telecom networks requires significant technical adjustments. Each telecom service provider (TSP) must update their infrastructure to support the new header format.

- **Standardization:** Ensuring uniformity in the format and usage of prefixes across different TSPs and regions can be complex. This requires coordination and agreement among multiple stakeholders.
- **Cost:** The implementation involves costs related to upgrading systems, training staff, and ongoing maintenance. Smaller TSPs might find it financially challenging to comply with these requirements.
- **User Awareness:** Educating consumers about the new system and how to interpret the prefixes is crucial. Without proper awareness, the benefits of the system might not be fully realized.
- **Regulatory Compliance:** Ensuring that all TSPs comply with the new regulations can be challenging. Continuous monitoring and enforcement are necessary to maintain the system's integrity.
- **Privacy Concerns:** There might be concerns about privacy and data security, as the system involves tracking and identifying the origin of messages. Ensuring that consumer data is protected is paramount.
- **Scalability:** As the number of telecom users and messages increases, the system must be scalable to handle the growing volume without compromising performance.

Despite these challenges, the benefits of increased transparency, accountability, and reduced spam make it a worthwhile endeavour.

Permitting the Sender to use the same numeric header for both messages and transactional/service voice calls, rather than a prefix system, has its own set of advantages and challenges:

Advantages:

1. **Consistency:** Having the same numeric header for both messages and calls creates consistency. Consumers can quickly recognize the

sender across different types of communication, which can enhance trust and reduce confusion.

2. **Ease of Recognition:** It simplifies the identification process for consumers. They don't have to remember different prefixes or codes for different types of communication from the same sender, making it easier to recognize legitimate communications.
3. **Streamlined Communication:** Businesses and service providers can maintain a unified identity across all communication channels, which can be beneficial for branding and consumer recognition.
4. **Reduced Complexity:** A unified numeric header system is simpler to implement and manage for both providers and regulators, potentially reducing the chances of errors or miscommunication.

Challenges:

1. **Reduced Differentiation:** Without a prefix system, it may be harder for consumers to differentiate between the types of communication (e.g., promotional vs. transactional) unless clearly indicated within the content.
2. **Increased Risk of Fraud:** If the same header is used for both messages and calls, it could potentially be exploited by fraudsters to mimic legitimate communications more effectively, leading to a higher risk of phishing or other scams.
3. **Lack of Transparency:** A prefix system inherently provides more information about the nature of the communication. Removing it could reduce transparency, making it more difficult for consumers to immediately assess the relevance or importance of the communication.

4. **Regulatory Challenges:** Regulators may find it more difficult to enforce rules and monitor compliance without distinct identifiers for different types of communication.

Conclusion:

While allowing the same numeric header for both messages and transactional/service calls offers benefits in terms of consistency and simplicity, it also comes with increased risks, particularly concerning fraud and transparency. Whether this approach is better than a prefix system depends on the specific goals of the communication policy and the consumer protection framework in place. A hybrid approach, where consistency is maintained but with additional safeguards, could potentially offer the best balance.

Several countries have implemented systems similar to the prefix system for identifying the Access Provider and Service Area in telecommunications. Here are a few examples:

United States: The Federal Communications Commission (FCC) mandates that telecommunication providers use specific caller ID prefixes to identify the type of call, such as toll-free numbers (800, 888, etc.) and area codes that indicate the geographic origin of the call.

United Kingdom: Ofcom, the UK's communications regulator, requires that certain prefixes be used to identify different types of services, such as geographic numbers (01, 02), mobile numbers (07), and non-geographic numbers (08, 09).

Australia: The Australian Communications and Media Authority (ACMA) has a numbering plan that includes prefixes to identify different types of

the **Unsolicited Commercial Communication (UCC)** framework offers several benefits:

1. Immediate Response and Action:

- Real-time transfer ensures that complaints about unsolicited communications are addressed promptly, minimizing delays in handling violations of UCC regulations.

2. Efficient Complaint Management:

- It enables streamlined communication between the platforms, allowing for quicker identification, tracking, and resolution of complaints by the relevant operators.

3. Improved Consumer Protection:

- Faster complaint handling enhances consumer confidence, as issues related to unsolicited communications are dealt with promptly, leading to better protection of consumer rights.

4. Enhanced Regulatory Compliance:

- Operators can respond swiftly to complaints, reducing the likelihood of repeated violations and ensuring compliance with the Telecom Commercial Communications Customer Preference Regulations (TCCCPR).

5. Data Accuracy and Integrity:

- Real-time transfer helps maintain the accuracy and integrity of complaint data, reducing the risk of data loss or errors that could occur during delayed processing.

6. Better Monitoring and Reporting:

- Authorities can monitor the handling of complaints more effectively and generate real-time reports, improving oversight and enforcement of UCC regulations.

7. Operational Efficiency:

- The automation and integration between TAP and OAP reduce the need for manual interventions, leading to more efficient use of resources and lower operational costs.

This mechanism ultimately aims to create a more robust system for managing and mitigating the effects of unsolicited commercial communications, benefiting both consumers and regulatory bodies.

Challenges :

The real-time transfer of complaints from the Transactional Analytical Platform (TAP) to the Operator Action Platform (OAP) within the Unsolicited Commercial Communication (UCC) framework also presents several challenges:

1. System Integration and Compatibility:

- Ensuring seamless integration between TAP and OAP requires sophisticated technical infrastructure. Compatibility issues between different systems or platforms used by various operators can lead to delays or errors in complaint transfer.

2. Data Overload and Latency:

- Real-time data transfer can generate a significant volume of information that needs to be processed instantly. If the systems are not equipped to handle this load, it may result in latency, where complaints are delayed in reaching OAP, defeating the purpose of real-time transfer.

3. Technical Glitches and Downtime:

- Any technical malfunction, such as server downtime or connectivity issues, can disrupt the real-time transfer process, leading to backlogs and delayed complaint resolution.

4. Accuracy of Data Transfer:

- Inaccurate or incomplete data transfer can occur if the systems are not fully synchronized or if there are glitches in the real-time process, leading to mismanagement of complaints.

5. Resource Allocation and Cost:

- Implementing and maintaining a real-time transfer system requires significant investment in technology, infrastructure, and skilled personnel. Smaller operators might struggle with the financial and operational demands of such a system.

6. Security and Privacy Concerns:

- Real-time data transfer increases the risk of security breaches, where sensitive consumer information could be intercepted or mishandled during the transfer process. Ensuring robust encryption and data protection measures is crucial.

7. Scalability Issues:

- As the volume of complaints grows, the system must be scalable to handle increased demand without compromising performance. Scaling the system in real-time can be technically challenging and costly.

8. Regulatory Compliance and Monitoring:

- Ensuring that all operators adhere to regulatory standards during the real-time transfer process requires continuous monitoring and updates, which can be resource-intensive.

9. Discrepancies in Complaint Handling:

- Variations in how different operators handle complaints can lead to inconsistencies, making it challenging to maintain uniformity and fairness in the complaint resolution process.

10. **Training and Skill Requirements:**

- Personnel involved in managing the real-time transfer process must be adequately trained to handle the technology and troubleshoot any issues that arise, which can be a logistical challenge.

These challenges need to be carefully managed to ensure that the real-time transfer of complaints from TAP to OAP is effective, reliable, and beneficial in addressing unsolicited commercial communications.

Different Criteria to initiate action against individual subscriber and enterprise subscribers for UTM complaints :

Agree with the TRAI's Suggestions.

In the context of Unsolicited Telemarketing (UTM) complaints under the Telecom Commercial Communications Customer Preference Regulations (TCCCPR), different criteria are used to initiate action against individual subscribers and enterprise subscribers. These criteria generally involve the frequency, severity, and nature of violations. Here's an overview of these criteria:

1. Individual Subscribers:

- **Frequency of Complaints:**

- Action may be initiated if a certain threshold of complaints is received against an individual subscriber within a specific time frame (e.g., multiple complaints in a month).

- **Nature of the Violation:**
 - If the complaints involve serious breaches, such as repeated sending of unsolicited commercial communications (UCC) despite being registered on the Do Not Disturb (DND) list, stricter actions may be considered.
- **Warning System:**
 - Typically, a warning is issued after the first complaint. Continued violations can lead to further penalties, such as service disconnection or blacklisting.
- **Type of Communication:**
 - If the UCC is sent via a personal number rather than a registered telemarketer, the penalties may differ, with more stringent actions taken against the misuse of personal communication channels.

2. Enterprise Subscribers:

- **Volume of Complaints:**
 - Enterprise subscribers (business entities) may be subject to action if they generate a high volume of complaints, even if these complaints are dispersed across different time periods.
- **Pattern of Violations:**
 - A pattern of consistent non-compliance, such as ignoring consumer preferences or failing to obtain necessary consent for communications, can trigger enforcement actions.
- **Severity of Offenses:**
 - Enterprises involved in large-scale UCC violations, such as sending bulk unsolicited messages, face stricter penalties.

Severe breaches can lead to fines, suspension of services, or even legal action.

- **Compliance History:**

- An enterprise's history of compliance is taken into account. Repeated or intentional violations are treated more severely, with escalating penalties.

- **Registration Status:**

- If an enterprise is not registered as a telemarketer but is found to be engaging in UCC activities, it faces penalties not only for the UCC violations but also for operating without proper registration.

3. Common Criteria:

- **Regulatory Warnings:**

- Both individual and enterprise subscribers may receive formal warnings before further action is taken. These warnings are intended to encourage compliance and provide an opportunity to rectify the behaviour.

- **Escalating Penalties:**

- Penalties usually escalate with repeated offenses. Initial actions may include warnings or fines, but repeated violations can lead to service suspension, blacklisting, or legal proceedings.

- **Investigation and Evidence:**

- Actions are typically initiated after an investigation that confirms the validity of the complaints. The investigation includes examining call logs, message content, and other relevant evidence.

4. Legal and Financial Penalties:

- **Fines:**
 - Both individuals and enterprises may be subject to fines depending on the severity of the violation and the number of complaints received.
- **Service Disruption:**
 - In severe cases, services may be temporarily or permanently disconnected to prevent further violations.
- **Legal Action:**
 - For severe or repeated violations, especially by enterprises, regulatory bodies may pursue legal action to enforce compliance.

The action taken against individual or enterprise subscribers can be designed to enforce compliance with the TCCCPR regulations, protect consumer rights, and maintain the integrity of communication networks.

Provisions to initiate action against the Sender for making promotional calls from the series assigned for transactional/service calls :

To effectively address the misuse of phone number series assigned for transactional or service calls by senders who make promotional calls, specific provisions should be established. These provisions would ensure that such misuse is promptly identified, discouraged, and penalized. Here are some suggested provisions:

1. Strict Classification and Monitoring:

- **Number Segregation:**

- Ensure that number series assigned for transactional/service calls are strictly segregated from those meant for promotional calls. Regulatory authorities should maintain clear guidelines on the classification and use of number series.
- **Real-Time Monitoring:**
 - Implement real-time monitoring systems to detect any misuse of transactional/service number series for promotional purposes. Such systems should automatically flag deviations and notify the relevant authorities for further action.

2. Mandatory Registration and Consent:

- **Sender Registration:**
 - Require all entities using number series for transactional/service purposes to register these numbers with regulatory bodies. The purpose of the number must be clearly defined during registration.
- **Consumer Consent:**
 - Ensure that senders have explicit consumer consent for transactional/service communications. Promotional content sent through these channels without consent should be treated as a violation.

3. Escalation and Penalty Mechanisms:

- **Warning System:**
 - Implement a tiered warning system. First-time offenders should receive a formal warning, clearly outlining the breach and the potential consequences of continued violations.
- **Financial Penalties:**

- Impose substantial fines on senders found to be using transactional/service numbers for promotional calls. The fines should escalate with repeated offenses to deter persistent violators.
- **Service Disconnection:**
 - In cases of severe or repeated misuse, the sender's access to the number series should be temporarily or permanently revoked. This can include suspension of services or disconnection of the offending numbers.
- **Blacklisting:**
 - Maintain a blacklist of senders who repeatedly misuse number series. Entities on this list should face restrictions on registering new numbers or accessing communication services.

4. Complaint Handling and Redressal:

- **Dedicated Complaint Channels:**
 - Establish dedicated channels for consumers to report promotional calls made from transactional/service numbers. These channels should be easily accessible and responsive.
- **Investigation and Resolution:**
 - Upon receiving complaints, initiate a prompt investigation to verify the misuse. If the complaint is validated, take immediate action against the sender as per the established penalties.

5. Audit and Compliance Checks:

- **Regular Audits:**
 - Conduct regular audits of number series usage by telecommunication providers and enterprises to ensure

compliance with the guidelines. Random checks should be performed to identify any misuse.

- **Compliance Reporting:**

- Require entities to submit regular compliance reports detailing their use of transactional/service numbers. Non-compliance should trigger further scrutiny and potential penalties.

6. Public Awareness and Education:

- **Consumer Awareness Campaigns:**

- Launch campaigns to educate consumers about the distinction between transactional/service calls and promotional calls. Consumers should be aware of their rights and how to report misuse.

- **Sender Education Programs:**

- Provide educational resources to businesses and service providers on the appropriate use of number series. This should include information on the legal implications of misuse.

7. Legal and Regulatory Framework:

- **Clear Legal Definitions:**

- Define legal terms clearly within the regulatory framework, distinguishing between transactional, service, and promotional communications. This clarity will help in enforcement.

- **Enforcement Authority:**

- Empower regulatory authorities with the necessary legal authority to enforce these provisions, including the ability to levy fines, disconnect services, and pursue legal action against violators.

These provisions would create a robust framework for preventing and penalizing the misuse of number series intended for transactional and service communications, thereby protecting consumers and maintaining the integrity of communication channels.

Action against Senders for UTM Violation and misuse of Series assigned for Transactional/Service calls :

When a sender violates regulations related to Unsolicited Telemarketing (UTM) and misuses the number series assigned for transactional or service calls, it undermines consumer trust and breaches regulatory compliance. To address these violations, the following actions should be taken:

1. Warning and Notification:

- **Formal Warning:**
 - Issue a formal warning to the sender upon the first violation, clearly stating the nature of the breach and the consequences of further infractions.
- **Public Notification:**
 - Notify the public and affected consumers about the violation through appropriate channels, reinforcing the importance of vigilance against unsolicited and unauthorized communications.

2. Financial Penalties:

- **Fines for Violations:**

- Impose substantial fines on senders who misuse the number series for promotional purposes. The amount should reflect the severity and frequency of the violations.
- **Escalating Penalties:**
 - Increase the fines with each subsequent violation to deter repeat offenders. Persistent misuse should result in progressively higher penalties.

3. Service Suspension and Disconnection:

- **Temporary Suspension:**
 - Temporarily suspend the sender's access to the number series used in the violation, preventing further misuse. The duration of the suspension should correspond to the severity of the violation.
- **Permanent Disconnection:**
 - For repeated or egregious violations, permanently disconnect the offending number series and revoke the sender's ability to register new numbers for a defined period.

4. Blacklisting and Restriction:

- **Blacklisting:**
 - Add the sender to a blacklist maintained by regulatory authorities, restricting their access to telecommunication services. Blacklisted entities should face barriers to registering new number series.
- **Restriction of Privileges:**

- Limit the sender's ability to use transactional or service number series in the future, possibly requiring additional oversight or approval before they can regain access.

5. Legal Action:

- **Prosecution:**

- Pursue legal action against senders who commit severe or repeated violations. This could include criminal charges if the misuse is found to be deliberate and harmful on a large scale.

- **Civil Penalties:**

- In addition to fines, impose civil penalties that may include compensation for affected consumers or funding for regulatory enforcement efforts.

6. Revocation of Licenses and Permits:

- **License Revocation:**

- Revoke any licenses, certifications, or permits granted to the sender that allows them to operate in the telemarketing or telecommunications sector. This action should be reserved for the most serious or repeated violations.

- **Temporary Ban:**

- Impose a temporary ban on the sender's ability to operate within the industry, with the duration depending on the violation's severity.

7. Audit and Compliance Monitoring:

- **Mandatory Audits:**

- Require the sender to undergo mandatory audits of their communication practices, ensuring compliance with regulations. The findings of these audits should be submitted to the regulatory authority for review.
- **Ongoing Monitoring:**
 - Place the sender under increased monitoring for a specific period to ensure they do not commit further violations. This might involve regular compliance reporting and check-ins with regulatory bodies.

8. Consumer Redressal and Compensation:

- **Consumer Compensation:**
 - Mandate that the sender provides compensation to consumers affected by the misuse, especially if they suffered financial or personal harm due to the unsolicited communications.
- **Establishment of a Redressal Mechanism:**
 - Ensure that a clear and accessible redressal mechanism is in place for consumers to report violations and seek compensation.

9. Public Awareness and Education:

- **Public Disclosure:**
 - Publicly disclose the sender's violations, along with the actions taken, to deter others from similar practices. This transparency also reinforces consumer confidence in regulatory enforcement.
- **Education Campaigns:**

- Launch educational campaigns to inform businesses and the public about the legal requirements for using transactional/service number series and the consequences of misuse.

10. Collaboration with Telecommunication Providers:

- **Provider Penalties:**

- If telecommunication providers are found complicit in the misuse (e.g., failing to monitor the appropriate use of number series), impose penalties on them as well.

- **Provider Cooperation:**

- Work closely with telecommunication providers to ensure they actively monitor the use of number series and report any suspicious activity or misuse by senders.

These actions, when applied consistently and effectively, would help maintain the integrity of communication systems, protect consumers from unsolicited and unwanted promotional communications, and ensure compliance with telecommunication regulations.

Entertaining complaints from customers not registered on DL-Preferences :

Different countries have adopted various frameworks to address complaints about unsolicited commercial communication (UCC), even for customers not registered on "Do Not Call" (DNC) or "Do Not Disturb" (DND) lists. Here's a look at what some major countries are doing in this area:

1. United States (FCC and FTC Regulations)

- **Regulatory Body:** Federal Communications Commission (FCC) and Federal Trade Commission (FTC).
- **Key Legislation:**
 - **TCPA (Telephone Consumer Protection Act):** Governs telemarketing calls and robocalls.
 - **CAN-SPAM Act:** Regulates commercial email.
- **Complaints Process:** Even if a customer is not on the National DNC list, they can:
 - File complaints about unwanted marketing calls, robocalls, or spam texts with the FCC or FTC.
 - Use the FCC's online portal or hotline to register complaints.
- **Actions Taken:**
 - **Warnings and Fines:** Telemarketers violating the rules can face significant fines (up to \$43,792 per call/text under the TCPA).
 - **Blocking Robocalls:** Telecom carriers are encouraged to offer call-blocking services to reduce UCC.
- **Consent-Based System:** Marketers need express consent to send UCC, even to those not on the DNC list.

2. United Kingdom (Ofcom and ICO)

- **Regulatory Body:** Ofcom (telecom regulator) and the Information Commissioner's Office (ICO).
- **Key Legislation:**
 - **PECR (Privacy and Electronic Communications Regulations):** Controls direct marketing and UCC.
 - **GDPR:** Governs data protection and privacy, adding a layer of consent for direct marketing.
- **Complaints Process:**

- Customers can complain to the ICO about UCC even if they are not registered with the **Telephone Preference Service (TPS)**.
- Complaints can be filed online or via phone.
- **Actions Taken:**
 - **Fines:** Businesses found guilty of sending UCC without consent can face fines up to £500,000.
 - **Investigations and Enforcement:** The ICO investigates complaints and can impose sanctions on marketers, including barring them from further communications.
- **Opt-In Requirement:** Explicit consent is required before sending UCC, even for unregistered users.

3. Canada (CRTC – Canadian Radio-television and Telecommunications Commission)

- **Regulatory Body:** CRTC.
- **Key Legislation:**
 - **Canada's Anti-Spam Legislation (CASL):** Applies to unsolicited marketing emails, texts, and other electronic communications.
 - **Telecommunications Act:** Regulates telemarketing and UCC over phone calls.
- **Complaints Process:**
 - Consumers can file complaints with the **National DNCL** (Do Not Call List) system if they receive UCC, even if they are not registered on the DNCL.
 - CASL also allows consumers to report unwanted commercial electronic messages.
- **Actions Taken:**

- **Fines:** Violations can lead to penalties of up to CAD \$10 million for businesses and CAD \$1 million for individuals.
- **Consent Requirement:** Similar to other regions, businesses need explicit consent to send UCC, even to non-registered users.

4. Australia (ACMA – Australian Communications and Media Authority)

- **Regulatory Body:** ACMA.
- **Key Legislation:**
 - **Spam Act 2003:** Governs unsolicited electronic messages like emails and texts.
 - **Do Not Call Register Act 2006:** Manages telemarketing calls.
- **Complaints Process:**
 - Customers can complain about UCC even if they are not on the **Do Not Call Register**.
 - Complaints can be lodged via ACMA’s website or hotline.
- **Actions Taken:**
 - **Fines and Warnings:** Businesses sending unsolicited messages or calls without consent face penalties up to AUD \$2.1 million.
 - **Blocking UCC:** ACMA can instruct telecom companies to block numbers that consistently violate UCC regulations.
- **Consent-Based Marketing:** Marketers need prior consent for UCC, regardless of a user’s registration on the DNC list.

5. European Union (GDPR and ePrivacy Directive)

- **Regulatory Bodies:** Various national data protection authorities (e.g., CNIL in France, ICO in the UK).

- **Key Legislation:**
 - **ePrivacy Directive:** Focuses on electronic communications, including marketing.
 - **GDPR:** Requires clear, unambiguous consent for processing personal data, including sending UCC.
- **Complaints Process:**
 - Any individual, regardless of their registration with a DNC list, can file complaints about UCC with their national data protection authority.
 - Complaints can be filed online, via phone, or in writing.
- **Actions Taken:**
 - **Fines:** Violations of the GDPR can lead to fines up to 4% of a company's global turnover or €20 million, whichever is higher.
 - **Investigations:** Data protection authorities can investigate and restrict companies from further communications.
- **Opt-In Consent:** Companies must obtain explicit consent for UCC, with easy options for users to withdraw consent.

6. India (TRAI – Telecom Regulatory Authority of India)

- **Regulatory Body:** TRAI.
- **Key Legislation:**
 - **TCCCPR 2018** (Telecom Commercial Communications Customer Preference Regulations): Regulates UCC.
- **Complaints Process:**
 - Consumers can complain about UCC even if they are not on the DND list via SMS or online portals.
- **Actions Taken:**

- **Warnings and Fines:** Telemarketers violating regulations face escalating penalties, from warnings to significant fines.
- **Blocking Repeat Offenders:** Persistent offenders are blocked from sending further UCC.

7. Singapore (PDPC – Personal Data Protection Commission)

- **Regulatory Body:** PDPC.
- **Key Legislation:**
 - **Do Not Call (DNC) Registry:** Governs telemarketing and UCC regulations under the Personal Data Protection Act (PDPA).
- **Complaints Process:**
 - Customers can complain about UCC even if not registered on the DNC registry.
 - Complaints can be lodged via the PDPC’s website.
- **Actions Taken:**
 - **Fines:** Violations of the PDPA, including sending UCC without consent, can lead to fines of up to SGD \$1 million.
 - **Investigation:** PDPC investigates complaints and takes enforcement actions, including stopping further communications.

Key Takeaways:

- **Global Approach:** Most countries have strong legal frameworks to protect consumers from UCC, even for those not registered on DNC lists. Complaints mechanisms exist in nearly all major countries, and they follow consent-based marketing rules.

- **Penalties:** Financial penalties for violating UCC regulations can be substantial, with many countries enforcing escalating fines for repeat offenses.
- **Consent:** The common theme across countries is the emphasis on explicit, opt-in consent before sending UCC. Even if a consumer is not on a DNC list, consent rules apply.

This shows that global regulations are increasingly prioritizing consumer consent and providing accessible mechanisms for lodging complaints.

Rejection of complaints due to ‘Incomplete Information’ or ‘Insufficient UCC Description’ :

When complaints about Unsolicited Commercial Communication (UCC) are rejected due to "Incomplete Information" or "Insufficient UCC Description," it is crucial to handle them systematically to ensure customer satisfaction and regulatory compliance. Here are some suggestions :

1. Clear Guidelines for Complaint Submission

- **Educate Customers:** Customers should be clearly informed about what information is needed when submitting a UCC complaint, such as:
 - Date and time of the UCC (call/message).
 - Sender’s phone number or identifier.
 - A detailed description of the content of the message or call.
 - Any prior consent given (if relevant).
- **Pre-Submission Checks:** Implement a user-friendly online portal or mobile app where the system flags incomplete complaints before submission, ensuring all required fields are filled in.

2. Prompt Feedback on Rejection

- **Reason for Rejection:** If a complaint is rejected due to incomplete information or insufficient UCC description, the rejection notice should clearly state the reason. This gives customers the chance to rectify and resubmit the complaint.
- **Automated Messages:** Use automated messaging systems (email, SMS, app notifications) to notify users immediately about missing information, and guide them on how to fix it.

3. Simplify Resubmission Process

- **Allow Resubmission:** Customers should be allowed to amend and resubmit their complaints with the missing details. Simplifying the process will encourage more users to complete their complaints.
- **Save Partially Submitted Complaints:** Allow customers to save partially filled complaint forms and return to them later, minimizing the chances of incomplete submissions.

4. Customer Support Assistance

- **Helpline or Chat Support:** Provide access to customer support through helplines or chatbots to assist users in submitting complete complaints. These support channels can guide customers on the necessary details for a valid complaint.
- **Proactive Outreach:** For important but incomplete complaints, service providers may initiate follow-up communications (via call or email) to help users provide the missing details and refile their complaints.

5. Detailed Templates for Complaint Submission

- **Complaint Templates:** Offer predefined complaint templates (especially for SMS or email) that prompt users to include all necessary information about the UCC they are reporting.
- **Example Descriptions:** Provide example descriptions of UCC to help users understand what is expected in the "description" field, ensuring sufficient detail for the investigation.

6. Automatic Collection of UCC Details

- **Data Collection Tools:** Implement automatic systems that capture relevant complaint information (such as call logs, SMS metadata) at the time of submission. For example:
 - If a user files a complaint about an SMS, the system can automatically capture the sender's number and timestamp from the message.
 - Users could be prompted to forward the UCC directly to the complaints system, minimizing errors and incomplete details.

7. Allow Attachments

- **Support for Screenshots and Attachments:** Allow customers to attach screenshots, call logs, or message snapshots to their complaints. This can help verify and complete any missing UCC information, providing evidence of the communication.

8. Collaboration with Regulatory Bodies

- **Regulatory Flexibility:** Regulatory bodies should provide clear guidelines on the minimum required information for UCC complaints. Where possible, they should encourage flexibility in accepting

complaints, especially for first-time filers or cases where technical issues caused incomplete information.

9. Escalation Procedures

- **Escalate Complex Cases:** For complex cases where critical details are missing but the UCC complaint is valid, service providers should have an escalation procedure. Such cases should be escalated for investigation, even if some minor details are missing.
- **TSP Intervention:** Telecom Service Providers (TSPs) can play an active role in filling gaps based on their internal data (e.g., sender number, message logs) for complaints with insufficient UCC descriptions.

10. Data Retention for Verification

- **UCC Data Retention:** Ensure that UCC data (call logs, message metadata) is retained for a reasonable period to allow users to retrieve and add missing details even after initial submission. This can prevent complaints from being discarded unnecessarily due to incomplete information.

By implementing these measures, customers will have a more effective way to submit and amend their complaints, ensuring that valid complaints are not dismissed due to minor errors or omissions.

Challenges and Concerns:

1. Effectiveness of Enforcement:

- Despite the provisions, enforcement has been a challenge. The volume of UCC complaints remains high, suggesting that the measures might not be fully effective in deterring violators.

Some consumers also report delays in the resolution of their complaints.

2. **Consumer Awareness:**

- Many consumers are unaware of the complaint mechanisms or how to effectively use them. This limits the reach and effectiveness of the current provisions.

3. **Repeat Offenders:**

- Even with penalties, some telemarketers continue to violate the rules, indicating that the current penalties may not be a strong enough deterrent.

4. **Escalation of Complaints:**

- While TCCCPR provides for a time-bound resolution, consumers may need more robust mechanisms for escalating unresolved complaints, such as an independent ombudsman or a more empowered regulatory body.

Sufficiency of Current Provisions:

While the existing provisions are comprehensive and have introduced innovative solutions like blockchain, there are areas where improvements could be made to enhance the effectiveness of UCC management:

- **Stronger Penalties:** Increasing the penalties for repeat offenders and providing stronger enforcement mechanisms could deter violators more effectively.
- **Improved Consumer Education:** Enhancing awareness campaigns to inform consumers about their rights and how to use the complaint mechanisms could lead to better utilization of these provisions.

- **Ongoing Monitoring and Audits:** Regular monitoring and audits of the TSPs' and telemarketers' compliance with the regulations could help in reducing the instances of UCC.

In conclusion, while the provisions under TCCCPR 2018 are a significant step towards managing UCC, there is room for improvement in enforcement, consumer awareness, and penalties to ensure that consumer complaints are addressed more effectively and in a truly time-bound manner.

Challenges :

Implementing regulations for Unsolicited Commercial Communications (UCC) can be quite challenging. Here are some common issues:

Technological Limitations: Identifying and blocking UCC can be difficult due to the evolving tactics used by spammers, such as spoofing caller IDs and using multiple numbers.

Consumer Awareness: Many consumers are not fully aware of their rights or the complaint mechanisms available to them, leading to underreporting of UCC incidents.

Enforcement and Compliance: Ensuring that all telemarketers and businesses comply with the regulations requires significant resources. Non-compliance can be hard to track and penalize effectively.

Coordination Among Stakeholders: Effective implementation requires coordination between telecom operators, regulatory bodies, and law enforcement agencies, which can be complex and time-consuming.

International UCC: UCC originating from international sources can be particularly challenging to manage due to jurisdictional issues and the difficulty in tracing the origin of such communications.

Resource Constraints: Regulatory bodies may face resource constraints in terms of manpower and technology, which can hinder the timely resolution of complaints.

Addressing these challenges often requires a combination of technological advancements, increased consumer education, stricter enforcement mechanisms, and international cooperation.

Challenges - UCC from International Sources :

When Unsolicited Commercial Communications (UCC) originate from international sources, several unique challenges arise that make it more difficult to regulate and manage these communications effectively. These challenges include:

1. Jurisdictional Issues:

- **Cross-Border Enforcement:** National regulations like TCCCPR 2018 are limited to the geographical boundaries of the country. Enforcing rules on entities located outside the country is challenging due to the lack of jurisdiction over foreign companies and individuals.
- **Legal Barriers:** Different countries have different laws and regulations regarding commercial communications. Coordinating legal actions across borders can be complex and time-consuming.

2. Tracking and Attribution:

- **Anonymity and Spoofing:** International UCC often involves techniques like caller ID spoofing, where the true origin of the

message or call is masked. This makes it difficult to trace the source and take corrective actions.

- **Unreliable Data:** Information about the origin of international UCC may be incomplete or inaccurate, making it challenging to identify the responsible parties.

3. Lack of International Agreements:

- **Insufficient Cooperation:** There is often a lack of international agreements or protocols for managing and enforcing regulations against UCC. This lack of cooperation between countries hampers efforts to combat international spam.
- **Different Regulatory Standards:** Countries may have varying standards for what constitutes UCC, and this inconsistency makes it hard to apply a uniform approach to managing such communications.

4. Technology and Resource Limitations:

- **Advanced Techniques:** International UCC sources may use advanced technologies like bots, AI, and automated systems to send vast quantities of messages, making it difficult for traditional filtering and blocking mechanisms to keep up.
- **Resource Constraints:** Telecom regulators and service providers may lack the resources or technological capabilities to effectively monitor and block UCC originating from multiple international sources.

5. Economic Incentives for Offenders:

- **Cost Advantage:** Sending UCC from international sources is often cheaper for spammers, especially if they exploit VoIP technology or

other low-cost communication channels. This economic advantage incentivizes the continued use of international routes for UCC.

- **Low Risk of Penalties:** Because of jurisdictional and enforcement challenges, offenders operating internationally often face a lower risk of penalties compared to domestic violators, encouraging more international UCC.

6. Impact on Consumers and Businesses:

- **Higher Fraud Risks:** International UCC is often associated with fraudulent schemes, such as phishing and financial scams, which can lead to significant losses for consumers and businesses.
- **Reduced Consumer Trust:** The influx of international UCC can erode consumer trust in legitimate communications from abroad, leading to a broader reluctance to engage with foreign entities.

7. Inadequate Consumer Awareness:

- **Lack of Knowledge:** Consumers may be less aware of how to identify and report international UCC, leading to underreporting and a slower response from regulatory bodies.

Potential Solutions:

- **International Cooperation:** Enhancing cooperation between countries through treaties, agreements, and information-sharing protocols to better regulate and manage international UCC.
- **Advanced Technology:** Implementing advanced AI-driven solutions to detect and block spoofed numbers and international UCC at the network level.

- **Global Standards:** Working towards global standards for commercial communications that can be adopted across jurisdictions to create a more unified approach to combating UCC.
- **Consumer Education:** Increasing consumer awareness about the risks of international UCC and how to report it effectively.

While addressing UCC from international sources is challenging, a combination of enhanced international collaboration, advanced technological solutions, and better consumer education can help mitigate these issues.

Technical Limitations in identifying and Blocking UCC :

Identifying and blocking Unsolicited Commercial Communications (UCC) involves various technical challenges due to the evolving methods used by spammers and the inherent limitations of current technologies. Here are some of the key technical limitations:

1. Caller ID Spoofing:

- **Definition:** Spoofing involves faking the caller ID to make it appear as if the call or message is coming from a legitimate or local source, even though it originates elsewhere.
- **Challenge:** This makes it difficult for telecom networks to identify the true source of the communication, complicating efforts to block UCC effectively. Spoofed IDs often bypass basic filtering mechanisms, leading to higher rates of successful UCC delivery.

2. Dynamic and Randomized Sender Information:

- **Rotating Numbers:** Spammers often use a large pool of phone numbers or dynamically generate new numbers for each message or call. This prevents telecom providers from creating effective blacklists, as blocking one number doesn't stop future communications from different numbers.
- **Randomized Sender IDs:** In the case of SMS or email, senders might use randomized alphanumeric codes, making it challenging to maintain an updated and effective blacklist.

3. Encrypted Communications:

- **Use of Encryption:** Some UCC may be transmitted through encrypted channels, making it difficult for telecom providers to inspect the content and determine whether it is spam or not.
- **End-to-End Encryption:** While beneficial for privacy, end-to-end encryption limits the ability of service providers to monitor and filter out UCC at the network level.

4. Advanced Content Obfuscation Techniques:

- **Text Manipulation:** Spammers often manipulate the text in their messages to avoid detection by filters. For example, they may replace certain letters with numbers or special characters (e.g., "Offer" instead of "offer"), which can evade keyword-based filtering systems.
- **Image-Based Spam:** UCC may also be sent as images (e.g., in MMS or emails) rather than text, making it harder for traditional text-based spam filters to detect and block.

5. Volume and Scale:

- **High Volume:** UCC is often sent in massive volumes, overwhelming existing filtering and blocking mechanisms. Handling and analyzing such large quantities of data in real-time can strain the resources of telecom providers.
- **Distributed Attacks:** UCC can originate from multiple sources globally, making it difficult to implement a centralized blocking strategy.

6. Network Latency and Real-Time Processing:

- **Real-Time Detection:** Identifying and blocking UCC in real-time is technically challenging, especially in high-traffic networks. Any delay in detection could result in the message or call reaching the recipient before it can be blocked.
- **Latency Issues:** Implementing sophisticated filters can introduce latency, which can negatively affect the quality of service for legitimate communications.

7. Insufficient Data and Context:

- **Contextual Understanding:** Many current systems rely on simple heuristics, such as keyword matching, which do not take into account the context of the communication. This can lead to both false positives (legitimate communications being blocked) and false negatives (UCC slipping through).
- **Limited Historical Data:** Lack of sufficient historical data on UCC patterns can reduce the effectiveness of machine learning algorithms designed to detect spam.

8. Bypassing DND (Do Not Disturb) Lists:

- **Exploitation of Exceptions:** Some UCC exploit exceptions in the DND registry (e.g., transactional messages or messages from government agencies), which can be abused by spammers pretending to be legitimate entities.
- **International Numbers:** Spammers may use international numbers to bypass local DND regulations, as such communications may not be adequately covered by local DND lists.

9. Fragmented Technological Ecosystem:

- **Diverse Systems:** The variety of telecom technologies and protocols across different networks (e.g., 2G, 3G, 4G, 5G) can make it difficult to implement uniform blocking measures.
- **Legacy Systems:** Older telecom infrastructure may not support modern filtering and blocking technologies, making some parts of the network more vulnerable to UCC.

10. Artificial Intelligence Evasion:

- **AI-Based Spam:** As telecom providers adopt AI for detecting UCC, spammers also use AI to evade detection, creating content that mimics legitimate communication or rapidly changes patterns to outsmart AI filters.
- **Adaptive Techniques:** Spammers continually adapt their techniques based on the AI's learning models, which requires constant updates and improvements in filtering systems.

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 complaints? Please provide your answer with full details on the facilities needed.

Comments :

The facilities extended by telecom service providers (TSPs) through **apps, websites, and call centers** for handling Unsolicited Commercial Communication (UCC) complaints are crucial in ensuring consumer protection and satisfaction. However, their effectiveness depends on several factors like accessibility, user-friendliness, and responsiveness. Here's an assessment of these facilities:

1. Mobile Apps for UCC Complaints

- **Accessibility:** Most major telecom providers have integrated UCC complaint handling features into their apps, making it convenient for users to lodge complaints from their smartphones. Many apps allow users to:
 - **Report UCC directly:** Forward unwanted SMS or report calls within the app.
 - **Check Complaint Status:** Users can track their complaints easily.
- **User-Friendly Design:** The design and ease of navigation in apps vary by provider. An ideal app:
 - Should have a **simple interface**, with easy-to-follow steps for filing complaints.

- Should minimize the information the user needs to input manually, for example by auto-fetching sender details from SMS or call logs.
- **Challenges:**
 - **Compatibility Issues:** Some apps may not be optimized for all devices or may require regular updates, which could hinder accessibility for certain users.
 - **Data Connectivity:** Users in areas with poor internet connectivity may face difficulties in accessing app features.
 - **Language Support:** Apps may not always offer multi-language support, limiting accessibility for non-English speakers or those preferring regional languages.

2. Websites for UCC Complaints

- **Accessibility:** Telecom service providers typically offer web portals where users can submit UCC complaints. Websites offer:
 - **Broader access:** Users can log in from any internet-enabled device.
 - **Submission Forms:** Most providers offer online forms to report UCC by entering details like the sender's number and the content of the message.
- **User Experience:**
 - **Ease of Use:** The websites should provide **clear instructions** on how to file a complaint and what details are necessary. Ideally, they should include **step-by-step guidance**.
 - **Form Design:** Forms should allow users to submit relevant information (like attaching screenshots or logs) and ensure that

error messages or missing details are flagged before submission.

- **Mobile Responsiveness:** Websites should be optimized for mobile browsers, making them as accessible as apps for users who prefer not to install apps.
- **Challenges:**
 - **Cluttered Interfaces:** Some websites might be overly complex, making it hard for users to navigate to the correct section for UCC complaints.
 - **Security Concerns:** Users might hesitate to use web portals for privacy or security reasons, especially if they handle sensitive personal information.
 - **Limited Support Options:** Not all websites provide comprehensive live chat or instant support for users facing difficulties during the complaint submission process.

3. Call Centers for UCC Complaints

- **Accessibility:** Call centers offer a more traditional and direct method for customers to file UCC complaints. This is especially useful for:
 - **Non-tech-savvy users:** Who may find apps and websites difficult to use.
 - **Areas with low internet access:** Where mobile data connectivity is poor or unavailable.
- **Ease of Use:**
 - **Personalized Help:** Users can explain their issues directly to a representative, ensuring the correct information is gathered and submitted.

- **Language Support:** Call centers usually offer multiple language options, catering to a broader range of consumers, including those in rural or regional areas.
- **Challenges:**
 - **Wait Times:** Long hold times or delays in connecting to a live representative can frustrate customers.
 - **Inconsistent Knowledge:** Some call center agents may not be well-trained or familiar with UCC complaint procedures, leading to incorrect information or poor customer service.
 - **Limited Hours of Operation:** If the call center isn't available 24/7, users may face difficulties filing complaints outside working hours.

4. User Feedback and Improvements

- **Consumer-Friendly Practices:**
 - **Simplified Steps:** Apps, websites, and call centers should offer **step-by-step processes** that make it easy for users to submit complaints with minimal effort.
 - **Transparency:** Providing real-time updates on complaint status via notifications or emails boosts consumer confidence in the system.
 - **Multi-Channel Support:** Allowing users to switch between channels (app, website, call center) to manage their complaints enhances accessibility.
- **Areas for Improvement:**
 - **Integration Across Channels:** TSPs should integrate data across all platforms (apps, websites, call centers) to provide seamless transitions for users who move between channels.

- **Better Awareness Campaigns:** Many consumers are unaware of the UCC complaint mechanisms available. TSPs could improve outreach through campaigns, SMS reminders, or app notifications explaining the complaint process.
- **Accessibility for Differently-Abled Users:** Apps and websites should be designed with features like **voice assistance, screen readers, and larger text** to cater to differently-abled users.

5. Overall Assessment

- **Accessibility:** In general, service providers offer accessible platforms for handling UCC complaints, with multiple options (apps, websites, call centers) to cater to a wide range of users.
- **User-Friendliness:** While many apps and websites are easy to use, there can be significant variation in quality, with some platforms being more intuitive than others.
- **Gaps:**
 - **Tech Accessibility:** Those without smartphones or consistent internet access might still find apps and websites challenging, making call centers essential.
 - **Training and Support:** Some call center agents may lack the necessary training to handle UCC complaints efficiently, leading to inconsistencies in service quality.

Recommendations for Improving Consumer-Friendliness:

1. **Multi-Language Support:** Apps and websites should offer comprehensive language options to accommodate users from diverse linguistic backgrounds.

2. **Enhanced Usability for Mobile Sites:** Websites should be fully optimized for mobile use to provide a similar experience to apps.
3. **Simplify Complaint Process:** Implementing auto-detection of UCC data (like sender numbers from call/SMS logs) in apps and websites can reduce errors and make the complaint process faster.
4. **Reduce Call Center Wait Times:** By ensuring more staff are trained in handling UCC complaints, providers can reduce wait times and improve service quality.
5. **Awareness Campaigns:** Regular outreach to educate customers on how to use these facilities can enhance engagement and ensure more complaints are properly handled.

In summary, while the facilities offered by service providers for handling UCC complaints are generally accessible and user-friendly, there are areas where improvements in usability, customer support, and consumer awareness could make the process smoother and more effective.

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 complaints?

Comments :

To ensure that **apps, websites, and call centers** are easily accessible to consumers for registering and tracking **Unsolicited Commercial Communication (UCC) complaints**, service providers should adopt several measures. These measures should focus on enhancing usability, accessibility, transparency, and efficiency. Here are the key actions that should be taken:

1. Simplified User Interface and Process

- **Easy Navigation:** Apps and websites should have a **clear, intuitive interface** with easily identifiable sections for filing and tracking UCC complaints. A well-organized menu should direct users to the complaint section without any unnecessary steps.
- **Minimal Information Input:** Automate the extraction of information such as the sender's number, date, time, and content of the UCC from users' call logs or SMS, reducing the need for manual entry.
- **Step-by-Step Guidance:** Provide **guided prompts** and **pre-filled complaint templates** that automatically include necessary details, ensuring a smooth complaint-filing process.
- **Pre-Submission Checks:** Implement validation mechanisms that check for missing or incorrect information before allowing the user to submit the complaint, reducing rejections due to incomplete data.

2. Comprehensive Multi-Channel Accessibility

- **Multi-Platform Support:** Ensure that apps, websites, and call centers are accessible across multiple devices (smartphones, tablets, desktops) and operating systems (iOS, Android, etc.).
- **Mobile App Optimization:** Mobile apps should be **lightweight** and work smoothly in areas with low connectivity or older devices. They should also be frequently updated for optimal performance.
- **Mobile-Responsive Websites:** Websites should be fully responsive, meaning they adjust to various screen sizes and work well on mobile devices, providing a similar experience to apps.
- **Multilingual Support:** Both apps and websites should offer **multi-language support**, especially in countries with diverse linguistic

populations. This ensures that non-English speaking users or those who prefer regional languages can file complaints comfortably.

3. Customer-Friendly Call Centers

- **24/7 Availability:** Call centers should be available **24/7**, especially for regions with less internet penetration, ensuring that customers can file complaints at any time.
- **Efficient Call Routing:** Reduce hold times and call center congestion by implementing efficient call-routing systems that prioritize UCC complaint calls.
- **Training Call Center Agents:** Agents should be well-trained in handling UCC complaints, including guiding users on providing complete information and offering real-time updates on their complaint status.
- **IVR Options for UCC Complaints:** The Interactive Voice Response (IVR) system should have a clear option for **UCC complaints** early in the menu, so users can easily access it without navigating complex layers.

4. Tracking and Time-Bound Disposal

- **Real-Time Complaint Tracking:** Provide users with **real-time tracking options** via apps, websites, and SMS notifications. Users should be able to log in and check the status of their complaints at any time.
- **Automated Updates:** Send automated SMS, email, or app notifications to customers at key stages (e.g., complaint received, under review, resolved) to keep them informed.

- **Complaint ID Generation:** Generate a unique **complaint ID** for each submission that can be easily tracked across all platforms (apps, websites, and call centers).
- **Clear Resolution Timeline:** Provide a **clear timeline** for resolving complaints, informing users how long the investigation might take and when they can expect resolution.
- **Escalation Mechanism:** Allow users to escalate their complaints automatically if they are not resolved within the specified time frame. Escalation options should be prominently displayed in the app and website.

5. Data Privacy and Security

- **Secure Communication:** Ensure all communication related to UCC complaints is **encrypted and secure** to protect the privacy of users' personal data.
- **Opt-In Consent for Complaint Tracking:** Users should be allowed to opt into regular tracking updates via SMS or email, ensuring they are always aware of the status of their complaints.

6. User Education and Awareness

- **User Tutorials:** Provide **step-by-step tutorials** and FAQs within the app and website to help users understand how to file complaints and track them. These could be in the form of **videos, illustrated guides,** or **pop-up help boxes.**
- **Awareness Campaigns:** Conduct regular **awareness campaigns** (via SMS, emails, and social media) informing customers of the available channels (apps, websites, call centers) for filing UCC complaints. Educate consumers on how easy it is to register and track complaints.

- **Interactive Chatbots:** Implement **AI-powered chatbots** on websites and apps to assist users in real time, answering questions about the UCC complaint process, helping to file complaints, and tracking them.

7. Enhanced Usability for Differently-Abled Users

- **Assistive Technologies:** Ensure that apps and websites are compliant with accessibility standards like the **Web Content Accessibility Guidelines (WCAG)**. Features should include:
 - **Voice-Assisted Navigation:** Enable **voice controls** or integration with screen readers for visually impaired users.
 - **Large Text Options:** Provide options to increase text size and contrast for users with visual impairments.
 - **Simplified Interfaces:** For differently-abled users, include simplified versions of the app or website that offer **basic complaint filing features** with minimal steps.

8. Efficient Backend and Complaint Processing System

- **Integration with DND Databases:** Ensure that apps and websites are linked to the **Do Not Disturb (DND)** database, so complaints can be processed quickly for users who are registered but still receive UCC.
- **Automation in Complaint Handling:** Use automation tools to **filter and categorize complaints**, making it easier for service providers to assign and resolve issues more quickly.
- **Data Analytics for Complaint Resolution:** Leverage **data analytics** to monitor patterns of UCC and identify repeat offenders, allowing for quicker resolution and enforcement actions.

9. Collaboration with Regulatory Authorities

- **Coordination with TRAI** : Service providers should coordinate with telecom regulators to ensure that UCC complaints are handled within the legal timeframe. This can be achieved by:
 - Sharing periodic reports on complaint resolution status.
 - Working with regulators to impose penalties on violators.

10. User Feedback and Continuous Improvement

- **Feedback Mechanism**: After resolving complaints, request user feedback via apps, websites, or calls to assess the satisfaction with the complaint handling process. Use the feedback to improve services.
- **Frequent Updates and Upgrades**: Regularly update apps and websites to fix bugs, improve user interfaces, and introduce new features based on user needs.

Summary of Actions:

- **Simplify Interfaces**: Provide easy-to-navigate apps and websites with minimal input requirements and automated complaint submission.
- **Real-Time Tracking**: Offer real-time tracking, regular notifications, and clear resolution timelines.
- **24/7 Multi-Channel Support**: Ensure accessibility via apps, websites, and 24/7 call centers, with well-trained agents.
- **Security and Privacy**: Protect user data with encryption and secure complaint submission.

- **User Awareness:** Conduct awareness campaigns and offer tutorials to educate users on the complaint process.
- **Accessibility for Differently-Abled Users:** Implement assistive technologies and simplified interfaces for all users.

By adopting these measures, service providers can ensure that their platforms are consumer-friendly, accessible, and efficient in handling UCC complaints, leading to timely resolutions and increased consumer trust.

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

Comments :

To further simplify and expedite the processes for **complaint registration, preference registration, and consent management** regarding **Unsolicited Commercial Communication (UCC)**, service providers can adopt additional innovative modes. These modes should be easy to use, quick, and accessible to all types of users, ensuring wider adoption and improved customer experience.

Here are some suggested methods:

1. SMS-Based Registration

- **Complaint Registration:** Allow users to register UCC complaints directly by sending a specific format SMS to a designated number (e.g., TRAI's 1909 in India). This could involve:

- Users forwarding the offending message or entering details of the unsolicited call (e.g., "COMP <Sender Number> <Time> <Short Description>").
- Simplifying the message format for complaints so users can submit it quickly.
- **Preference and Consent Management:**
 - Enable users to **register or update their DND preferences** and manage their **consent** for specific categories of communications through simple SMS commands (e.g., "PREF <Category On/Off>" or "CONSENT <Brand On/Off>").
 - Provide users with confirmation messages and a summary of their preferences after submission.

2. USSD Codes (Unstructured Supplementary Service Data)

- **Complaint Registration:** Similar to how balance inquiries or data usage are checked, USSD codes could allow users to register UCC complaints quickly without the need for internet access.
 - Example: Users dial a specific code like ***123*1#** and follow the on-screen prompts to file their complaint by entering the sender's number or details of the UCC.
- **Preference and Consent Registration:** USSD codes can also enable users to register their DND preferences or manage their consents, especially for users without smartphones or internet connections. The interface can offer simple options like:
 - ***123*2#** for DND preferences.
 - ***123*3#** for consent management (granting or revoking permissions for specific promotional categories).

3. IVR (Interactive Voice Response) System

- **Complaint Filing via IVR:** Enhance the IVR systems to allow users to file UCC complaints with voice prompts. The system could:
 - Ask users to **input the sender's number** or provide a description of the UCC message/call.
 - Give users options to **record their complaint** if they prefer voice input.
- **Preference and Consent Registration:** Similarly, IVR systems could:
 - Provide options for users to **register DND preferences** or **update consents** through a series of easily navigable voice prompts, allowing users to select specific categories of communication they want to opt into or out of.
 - Offer **multilingual support** to cater to diverse demographics.

4. Social Media and Messaging Apps Integration

- **Complaint Registration via WhatsApp/Telegram/Other Messaging Apps:**
 - Service providers can integrate their complaint systems with popular messaging platforms like **WhatsApp, Telegram, or Facebook Messenger**, allowing users to file complaints by:
 - Forwarding UCC messages.
 - Using a chatbot interface where users answer prompts or fill in the required details.
 - The chatbot could offer real-time updates on complaint status as well.
- **Preference and Consent Registration:**

- Users can interact with the chatbot to set or change their preferences and manage consents by selecting categories from a menu.
- These platforms are widely used and familiar to most users, offering a seamless and quick registration process.

5. Voice Assistants (Alexa, Google Assistant, Siri)

- **Complaint Registration:** Integration with **voice assistants** like **Amazon Alexa, Google Assistant, or Siri** would enable users to register UCC complaints using voice commands. For example:
 - Users could say, “Alexa, file a UCC complaint” or “Google, register a spam call complaint,” and follow the voice prompts to provide the necessary information (such as the sender’s number).
- **Preference and Consent Registration:**
 - Similar voice commands can allow users to manage their DND preferences and consents, such as “Alexa, block all promotional calls” or “Google, allow health-related promotional messages.”
- This method is particularly convenient for **tech-savvy users** who prefer voice-enabled interaction over typing.

6. Mobile App Shortcuts and Widgets

- **Quick Complaint Submission via App Widgets:** Service providers could enhance their mobile apps by creating:
 - **Widgets** that allow users to quickly report UCC without navigating through the app’s full interface. A single tap on the

widget can forward a message or prompt users to enter complaint details.

- **Shortcuts** on the home screen of the app that directly open the complaint submission page or DND preference settings, reducing the steps needed for users to register complaints or manage consents.
- **Push Notifications for Consent Management:** Apps could send **push notifications** periodically reminding users to review or update their consent settings. With a single tap on the notification, users can review and manage all their permissions.

7. QR Code-Based System

- **Complaint Registration via QR Code:** Telecom providers could display **QR codes** (on their bills, websites, or promotional materials) that link directly to complaint registration pages or apps. Users can simply scan the QR code using their smartphone camera to open a pre-filled complaint form.
- **Preference and Consent Registration:** Similarly, QR codes could be used to redirect users to **preference registration** or **consent management** portals, making it faster to access these features.

8. Email-Based Registration

- **Complaint and Consent Management via Email:**
 - For users who prefer using email, service providers can create **dedicated email addresses** for UCC complaint registration. Users can forward UCC messages or describe unsolicited calls in an email format.

- An automatic reply system should acknowledge the complaint and provide a tracking number.
- For preference and consent registration, users could email specific formats (e.g., “PREF <On/Off> <Category>”) to modify their preferences.

9. Simplified Web Widgets or Extensions

- **Web Browser Extensions:** Users who spend a lot of time on desktop browsers can use browser extensions to quickly file UCC complaints or manage preferences. A small button or icon could appear in the browser interface, enabling users to submit complaints with a few clicks.
- **One-Click Consent Management:** Extensions or website widgets could offer one-click buttons for consumers to opt in or out of marketing communication preferences quickly.

10. Contactless UCC Reporting (e.g., NFC Technology)

- **NFC-Enabled Complaint Registration:** For users with NFC-enabled smartphones, service providers could offer NFC tags (placed in stores or on bills). Users tap their phones on the NFC tag, which opens the UCC complaint form or preference registration page instantly.

11. Public Self-Service Kiosks

- **Physical Kiosks in Public Places:** Service providers could place **self-service kiosks** at popular locations (like shopping malls or telecom retail outlets) where users can file UCC complaints or manage preferences by simply entering their phone numbers and selecting options on the screen.

12. Automated Voice Callbacks for Consent/Preference Management

- **Automated Consent Review Calls:** Service providers can initiate **automated voice callbacks** periodically, asking users to confirm or update their marketing preferences and consent. Users can interact with the voice prompts and choose which categories to block or allow.
- **Quick Complaint Registration:** An automated callback could also be triggered to assist users who are unable to register a UCC complaint initially, guiding them through the process and recording their response.

Summary of Additional Modes:

- **SMS/USSD Codes:** For simple, text-based interaction without requiring the internet.
- **IVR:** Accessible to all, with voice prompts for easy navigation.
- **Messaging Apps:** Leveraging popular apps like WhatsApp for complaints and consent management.
- **Voice Assistants:** Using Alexa, Google Assistant, or Siri for quick voice commands.
- **App Widgets:** One-tap complaint registration or preference settings from the home screen.
- **QR Codes:** Scanning for direct access to complaint or consent management pages.
- **Browser Extensions:** Quick submission via desktop.
- **Public Kiosks:** Physical touchpoints in retail or public spaces for easy access.

These modes, if implemented, would cater to a diverse range of consumers, offering convenient and user-friendly methods to manage UCC

complaints and consent preferences, thereby enhancing the overall customer experience.

Other Countries are employing innovative approaches to make unsolicited commercial communication (UCC) complaints, preference registrations, and consent handling more accessible and consumer-friendly. Here are some additional methods that have been implemented globally:

1. **Simplified Mobile and Web Portal Interfaces:** Countries like India have emphasized user-friendly design in mobile apps and web portals. Providers are required to display easy-to-find options for complaints, preference registration, and consent management. For example, apps often pre-populate details such as sender information for UCC complaints to minimize user input effort, provided the user consents to share such data.
2. **Voice Commands and Interactive Voice Response (IVR):** Countries such as the U.S. and India are increasingly adopting voice command options via IVR systems to allow users to register complaints or set preferences without needing to navigate complex menus. This provides a simpler, faster alternative for users uncomfortable with digital platforms.
3. **Chatbot Integration:** Several countries are leveraging chatbots to handle basic complaint registrations, consent updates, and preference changes. This mode offers a quick and conversational way for users to interact with services without logging into portals or apps.
4. **SMS-based Registration:** Countries like South Africa offer SMS-based registration for complaints and preferences, where consumers can text short codes to register or change their preferences. This

method is particularly helpful for those who may not have access to smartphones or the internet.

5. **Real-Time Complaint Tracking:** Many countries, such as the U.K. and Australia, are introducing real-time complaint tracking, ensuring consumers can follow up on their UCC complaints and see resolution timelines through both mobile and web applications.

Implementing these additional modes enhances accessibility and convenience, helping more consumers quickly address UCC issues.

Audit of implementation of TCCCPR 2018 :

Apart from the aspects mentioned by the TRAI following aspects should be considered :

An audit of the implementation of the **TCCCPR 2018 (Telecom Commercial Communications Customer Preference Regulations)** should cover several key aspects to ensure compliance and effectiveness. Below are the primary areas that should be audited:

1. Regulatory Compliance

- **Registration of Telemarketers (TMs):** Ensure that all telemarketers have registered with the Distributed Ledger Technology (DLT) platform.
- **Header and Template Registration:** Verify if all TMs have registered their headers (Sender IDs) and message templates with the DLT platform.
- **Consent Management:** Check whether customer consents for receiving commercial communications are recorded and managed properly.

- **Consent Revocation Mechanism:** Ensure that customers can revoke their consent easily and that this is implemented effectively.

2. Message and Call Categorization

- **Promotional vs. Transactional Messages:** Ensure clear classification and adherence to regulations regarding the use of service categories (promotional, transactional, or service categories).
- **Scrubbing of Non-Compliant Messages:** Confirm that non-compliant messages and calls are scrubbed to prevent their transmission.
- **Block Unauthorized Promotional Communications:** Ensure that the mechanism for blocking unauthorized promotional messages and calls is functional.

3. Complaint Redressal Mechanism

- **Customer Complaints Handling:** Review the complaint management system for handling DND (Do Not Disturb) violations and other issues related to unsolicited commercial communication.
- **Resolution Timelines:** Check if complaints are resolved within the regulatory timeframes set by TCCCPR 2018.

4. DLT (Distributed Ledger Technology) Compliance

- **Data Integrity and Security:** Review the usage of DLT to ensure that data integrity and security requirements are being met, and ensure that customer data is not misused.
- **Traceability:** Ensure that all commercial communications are traceable to the source, and there is accountability in the case of violations.

5. Consent Acquisition and Validity

- **Verification of Consent Source:** Ensure the consent acquisition process is compliant with the regulations and that proper records are maintained.
- **Audit of Consent Validity:** Review if the consents are still valid, especially if they are being used for a prolonged period.

6. Telemarketer Penalties

- **Penalties for Violations:** Review the penalties imposed on telemarketers who violate TCCCPR norms. Ensure the penal system is effective and applied consistently.

7. Technology Upgradation and Adaptation

- **Use of Advanced Filtering Systems:** Ensure that telecom service providers (TSPs) are using the latest technology to detect and block spam, including AI/ML-based systems for fraud detection.
- **Periodic Upgrades:** Check if TSPs and telemarketers are upgrading their systems in line with new technologies and regulatory changes.

8. Compliance Reporting

- **Reporting Mechanism:** Ensure TSPs and telemarketers are regularly reporting compliance with TCCCPR 2018.
- **Audit Logs and Reports:** Verify that audit logs and reports are maintained, and discrepancies are flagged for further action.

By covering these areas in the audit, one can ensure a robust assessment of how effectively TCCCPR 2018 is being implemented across the telecom ecosystem.

Information to the Authority on real-time basis :

The **TRAI** should have **real-time access** to specific information across various processes and databases related to complaint handling and other operations to ensure compliance with regulations such as the **TCCCPR 2018** and other telecom frameworks. Below are the key types of information TRAI should access in real time:

1. Complaint Handling System

- **Complaint Registration Data:**
 - Information on complaints registered by consumers regarding unsolicited commercial communications (UCC), DND violations, service quality, billing issues, etc.
 - Date, time, and nature of the complaint (e.g., UCC, service quality, billing).
- **Complaint Resolution Status:**
 - Real-time tracking of the status of complaints, including pending, in-process, resolved, or escalated cases.
 - Resolution timelines and whether they adhere to prescribed timelines.
- **Customer Feedback on Resolution:**
 - Data on customer feedback and satisfaction post-resolution to ensure service quality.

2. Consent Database

- **Consent Management Records:**

- Access to real-time data of customer consents for receiving promotional or transactional communications, as recorded by telemarketers and telecom service providers (TSPs).
- Consent acquisition and revocation records, including timestamps and details of who acquired consent and under what circumstances.
- **Consent Revocation Data:**
 - Immediate updates on consent revocation by consumers, ensuring that their preferences are respected in real-time.

3. Distributed Ledger Technology (DLT) Data

- **Telemarketer Registration:**
 - Information on the registration status of telemarketers, including approved and blacklisted entities.
 - Headers and message templates registered by each telemarketer.
- **Message Templates:**
 - Real-time access to all pre-registered templates for messages (promotional, transactional, service-related) to ensure compliance with regulations.
 - Immediate flagging of unregistered or non-compliant templates.

4. Commercial Communication Data

- **UCC and DND Violations:**
 - Real-time information on the number and types of UCC violations detected by TSPs.

- Data on communications blocked for non-compliance with TCCCPR regulations, including source information (telemarketer or service provider).
- **Scrubbing of Non-Compliant Messages:**
 - Data related to the scrubbing process that ensures non-compliant messages (those without valid consent) are blocked before transmission.
 - Reports on unauthorized communication attempts.

5. Telecom Service Providers (TSP) Data

- **Telecom Network Performance:**
 - Access to real-time data on network performance, quality of service (QoS), and outages that may affect the ability of TSPs to meet regulatory requirements.
- **Fraud Detection and Prevention:**
 - Real-time access to fraud detection mechanisms used by TSPs, including AI/ML models for identifying spam and fraudulent calls or messages.
 - Reporting of suspicious or fraudulent commercial communications.

6. Penalties and Blacklisting Data

- **Penalty and Compliance Records:**
 - Data on penalties imposed on telemarketers or TSPs for violating TCCCPR regulations, including financial penalties and other punitive actions.
 - Blacklisted telemarketers and the reasons for blacklisting.

7. Complaint Analytics and Reports

- **Real-Time Analytics:**
 - Access to real-time analytics on trends in customer complaints, including region-wise or telemarketer-specific violations, recurrence rates, and systemic issues.
 - Identification of emerging patterns in complaints that may signal deeper regulatory or compliance gaps.

8. Do Not Disturb (DND) Database

- **DND Activation and Deactivation:**
 - Real-time access to records showing DND activation/deactivation status by customers.
 - Updates on whether promotional messages and calls respect these preferences.

9. Telemarketer Activity Monitoring

- **Telemarketer Communication Logs:**
 - Real-time access to communication logs of telemarketers, including the volume of messages and calls sent, categorized by type (promotional, transactional, service-related).
- **Promotional Campaign Details:**
 - Real-time details of ongoing promotional campaigns, including target audience, templates used, and consent status.

By having real-time access to these types of information, TRAI can ensure a proactive regulatory environment, monitor compliance, quickly address violations, and enhance overall customer experience.

Header Information to the Public :

Agree with TRAI.

To enable the public to identify the senders of unsolicited commercial communications (UCC), telecom service providers (TSPs) should provide specific header information that makes it easy to trace the sender and the nature of the message. As per the **TCCCPR 2018** guidelines, the type of header information service providers should make available to the public includes:

1. Sender ID (Header) Information

- **Alphanumeric Headers:**

- Headers, also known as Sender IDs, are alphanumeric codes (e.g., VM-XXXXXX or AD-YYYYY) used to identify the entity sending the message.
- The first two characters indicate the **service provider code** (e.g., VM for Vodafone Idea, AD for Airtel, etc.).
- The remaining characters (typically 5-6 digits/letters) identify the **telemarketer or enterprise** sending the message.
- This header helps consumers recognize whether the message is from an **authorized sender** and which service provider was used to transmit it.

2. Category of Communication

- **Promotional Headers:**

- These headers are used for promotional messages and typically contain a special identifier (such as "TM" for telemarketer or

other abbreviations) to indicate that the message is commercial or promotional in nature.

- For instance, a promotional message may have a header like "AD-BANK01," where "BANK01" represents a bank sending promotional offers.

- **Transactional Headers:**

- These headers are used for service-related or transactional communications, such as OTPs (One-Time Passwords), account updates, and booking confirmations. They must be distinct and not used for promotional purposes.
- An example might be "VM-BANK01" for a bank sending an OTP.

- **Service-Related Headers:**

- Service-related messages are non-promotional communications that deal with the provision of services, such as reminders, customer care updates, or notifications about ongoing services.
- These headers usually indicate the nature of the service being provided and the sender (e.g., "AD-SERV01").

3. Telemarketer Identification

- The header should help identify the **specific telemarketer** or entity that sent the message. This ensures transparency and accountability.
- Information regarding the telemarketer or entity sending the message should be available through public directories or provided by TSPs to enable recipients to track the sender.

4. Service Provider Code

- The public should be able to recognize the **originating service provider** (such as Airtel, Jio, Vodafone, etc.) based on the first two characters of the header.
- A guide explaining the mapping of service provider codes to their corresponding companies should be made available to the public.

5. DND and Complaint Information

- The header or message body should include information on how consumers can report unwanted messages or register a complaint (e.g., short codes like 1909 for DND complaints).
- Instructions on opting out of promotional communications should be provided, giving the public an easy way to revoke consent.

6. Time and Date of Communication

- **Timestamping** of the message (either through the header or elsewhere in the message) is crucial for tracking and auditing UCC.
- Real-time access to the **time and date** of the communication helps consumers and regulators track when the communication was sent and whether it violated time-bound restrictions (e.g., no promotional messages after 9 PM).

Summary of Key Header Information to Be Provided to the Public:

1. **Sender ID (alphanumeric)** indicating the telemarketer and service provider.
2. **Category of the message** (promotional, transactional, or service-related).
3. **Telemarketer or enterprise** details behind the message.

4. **Service provider code** indicating the TSP that transmitted the message.
5. **DND/complaint information** and opt-out instructions.
6. **Timestamp** of the communication (time and date).

Making this information accessible and easy to understand enables consumers to identify and act against unwanted communications while ensuring transparency and compliance with TCCCPR 2018.

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**

Comments :

Measures required for pro-active detection of spam messages and calls through honeypots :

Proactive detection of spam messages and calls through **honeypots** involves setting up systems specifically designed to attract and monitor unsolicited commercial communications (UCC). This enables the identification and analysis of spammers and their techniques. The following measures are required for effective detection:

1. Honeypot System Design and Deployment

- **Dedicated Numbers for Monitoring:** Deploy a series of phone numbers (both mobile and landline) designated solely for the purpose

of monitoring incoming calls and messages. These numbers are not linked to any real users but are designed to attract spam.

- **Varied Distribution of Numbers:** Honey pot numbers should be distributed across different regions, service providers, and even across different user categories (e.g., Do Not Disturb (DND)-activated numbers, non-DND numbers) to attract a wide range of spam messages and calls.

2. Automated Collection and Logging

- **Automated Logging of Messages and Calls:** All incoming messages and calls to the honey pot numbers should be automatically logged with details such as timestamp, message content, sender/caller ID, and type of communication (SMS, voice call, etc.).
- **Recording Voice Calls:** For spam calls, especially robocalls, recording the voice content is essential. This helps identify patterns in language, tone, or content used by spammers.

3. AI-Based Content Analysis and Classification

- **Natural Language Processing (NLP) for Message Content Analysis:** Implement NLP algorithms to automatically analyze the content of SMS messages. The system should be able to detect patterns of spam based on keywords, repeated content, and suspicious links.
- **Voice Analysis for Spam Calls:** Use voice recognition technology to analyze the content of calls. Patterns such as repetitive phrases, pre-recorded messages, or scripts can help flag calls as spam.

4. Behavioral Pattern Detection

- **Caller/Sender Behavior Analysis:** Monitor repeated attempts by the same numbers to send messages or make calls to multiple honeypot numbers. Frequent or large-scale messaging/calling activity from a single number can be a strong indicator of spam behavior.
- **Bulk Messaging Detection:** Implement a system to detect bulk SMS messages sent simultaneously or within a short time frame. This behavior is typical of spammers targeting multiple users at once.

5. Real-Time Monitoring and Alerts

- **Real-Time Data Processing:** Set up real-time monitoring tools to process incoming messages and calls instantly. This allows for immediate detection of spam and quick identification of spam networks.
- **Automated Alerts:** The system should generate automatic alerts when specific thresholds are met (e.g., a certain number of messages/calls from the same number within a given timeframe), flagging the activity as potentially suspicious.

6. Blacklist Generation and Sharing

- **Dynamic Blacklist Creation:** The honeypot system should maintain a dynamic blacklist of numbers identified as spammers. This list should be continuously updated and shared with telecom service providers and regulatory bodies to prevent spammers from operating.
- **Collaboration with Telecom Operators:** Establish real-time collaboration with telecom operators, ensuring that once a number is flagged by the honeypot, the operator can block or throttle communication from that number.

7. Link and Attachment Scanning

- **URL/Link Analysis:** For messages containing links, implement automatic URL scanning to detect malicious websites, phishing attempts, or harmful content.
- **Attachment Scanning:** If the spam message contains attachments (e.g., images, documents), these should be automatically scanned for viruses, malware, or malicious intent.

8. Machine Learning for Continuous Improvement

- **Adaptive Machine Learning Models:** Implement machine learning algorithms that can learn from the evolving nature of spam communications. As spammers adjust their methods, the system should adapt by recognizing new patterns and behaviors.

9. Periodic System Audits and Updates

- **Regular Audits:** Periodically audit the honeypot system to ensure that it is effectively attracting spam communications and functioning as intended.
- **Database Updates:** Continuously update the system's spam detection algorithms with new patterns, keywords, and behaviors derived from ongoing monitoring and reports from regulatory bodies like TRAI.

10. Compliance with Privacy and Legal Guidelines

- **Data Protection:** Ensure that the honeypot system complies with privacy regulations, such as ensuring that the logged data is not

misused or improperly accessed. Encryption of sensitive data is essential.

- **Legal Collaboration:** Work closely with legal and regulatory authorities to ensure that the system adheres to national laws regarding telecommunications and unsolicited communication.

By implementing these measures, a robust honeypot system can effectively detect, track, and prevent spam messages and calls, helping in the proactive identification and mitigation of spammers.

Norms for the deployment of Honeypots in a LSA :

The deployment of honeypots in a Licensed Service Area (LSA) for detecting unsolicited commercial communications (UCC) should be guided by norms that ensure their effective operation while maintaining privacy, security, and legal compliance. Below are key types of norms that should be established for such deployment:

1. Legal and Regulatory Compliance

- **Approval and Licensing:** Honeypots should be deployed in compliance with the licensing norms set by the Telecom Regulatory Authority of India (TRAI) and the Department of Telecommunications (DoT). Approval may be required before deploying honeypots in an LSA.
- **Compliance with TCCCPR 2018:** The honeypot deployment must adhere to the Telecom Commercial Communications Customer Preference Regulations (TCCCPR) 2018, which governs how unsolicited commercial communication is handled. The honeypot's operation should fall under the regulatory framework to avoid potential misuse or privacy violations.

- **Data Privacy Regulations:** Honeytrap systems must comply with national and regional data protection laws, such as the Information Technology Act and the Personal Data Protection Bill (if applicable). This includes ensuring that no sensitive personal information is captured or used without consent.

2. Deployment Scope and Design

- **Number and Distribution of Honeytraps:** A sufficient number of honeytrap numbers should be deployed across the LSA to capture a diverse set of spam activities. This distribution should take into account:
 - Different telecom service providers (TSPs) operating in the area.
 - Urban and rural populations to ensure wide coverage.
 - Different user categories (e.g., DND-registered and non-DND-registered).
- **Virtual and Physical Honeytraps:** Consider a combination of virtual honeytraps (deployed on cloud systems) and physical honeytraps (actual devices in different geographic regions of the LSA) to attract diverse types of spam communication.
- **Public and Private Honeytraps:** Honeytrap systems can be deployed with a mix of public (numbers exposed in public domains) and private (numbers not publicly listed) configurations. This approach helps to capture both mass spamming and targeted spam activities.

3. Security and Privacy Norms

- **Data Encryption:** All data collected by the honeytrap, including messages, call records, and metadata, should be encrypted to protect it from unauthorized access or cyber threats.

- **Anonymization of Collected Data:** Honeypots should be configured to avoid capturing personal data unnecessarily. If any personal data is collected (e.g., sender or caller ID), it should be anonymized before processing to comply with privacy laws.
- **Access Control:** Strict access control measures should be in place to limit who can view or analyze the data collected by the honeypot. Only authorized personnel should be able to access sensitive logs.

4. Monitoring and Reporting Norms

- **Automated Monitoring Systems:** Honeypots should be equipped with real-time automated monitoring systems that can quickly detect suspicious activity and provide instant alerts to regulatory bodies or telecom operators.
- **Periodic Reporting to Authorities:** Regular reports (e.g., weekly or monthly) of spam activities detected by the honeypot should be submitted to TRAI and relevant telecom operators in the LSA. These reports should include:
 - Frequency and type of spam messages or calls.
 - Patterns of repeated violations.
 - Identified or suspected sources of spam.

5. Collaboration with Telecom Service Providers (TSPs)

- **Real-Time Data Sharing with TSPs:** Honeypot systems should be integrated with telecom service providers operating in the LSA for real-time data sharing. TSPs should be able to block or restrict numbers flagged by the honeypot system immediately to minimize spam activities.

- **Cross-Operator Coordination:** Establish norms for collaboration between multiple telecom operators in the LSA to prevent spammers from switching between providers to avoid detection.

6. Data Retention and Disposal Policies

- **Data Retention Period:** Define a clear retention period for the data collected by honeypots. Typically, this period should balance operational needs and privacy considerations, such as 6 to 12 months, after which data should be securely deleted unless required for ongoing investigations.
- **Data Disposal:** Ensure secure disposal mechanisms for the data collected by honeypots to prevent any misuse after it is no longer required.

7. Quality Control and Performance Audits

- **Periodic Audits of Honeypot Effectiveness:** Honeypot systems should undergo regular audits to evaluate their effectiveness in detecting spam. This includes assessing:
 - The volume of spam detected.
 - Accuracy of the system in identifying false positives.
 - Responsiveness to emerging spam patterns.
- **Regular Updates to Algorithms:** The spam detection algorithms should be regularly updated based on audit findings and changes in spam techniques to ensure continued effectiveness.

8. Integration with National and Global Systems

- **National Spam Detection Framework:** Honeypots should be integrated with a national spam detection framework to facilitate

coordinated action across LSAs. This allows for a unified response to spam threats and prevents spammers from exploiting regulatory loopholes across different regions.

- **International Collaboration:** If applicable, honeypots should be aligned with international spam detection systems to deal with cross-border spam threats. Cooperation with global telecom bodies may help identify spammers operating internationally.

9. Accountability and Legal Framework

- **Accountability for Misuse:** Clearly define accountability measures in case of misuse of honeypot systems. If unauthorized personnel misuse the system to capture non-spam communications, there should be strict penalties and legal action.
- **Legal Framework for Spam Prosecution:** Establish norms for how data collected by honeypots can be used as legal evidence in prosecuting spammers. This may require coordination with law enforcement agencies to ensure the data's integrity in legal proceedings.

10. Public Awareness and Transparency

- **Public Disclosure of Policies:** Telecom authorities should provide clear public communication regarding the purpose and use of honeypots in detecting spam. Users should be made aware that the system exists to protect their communication rights.
- **Complaint Redressal Mechanism:** Establish a transparent redressal system for consumers who may suspect that their legitimate communication is being flagged by honeypots. This allows for checks on false positives and helps protect consumer rights.

By establishing these norms, honeypots in an LSA can function effectively as a tool for spam detection and reduction, while ensuring the system remains secure, compliant with legal standards, and respectful of privacy.

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 :

For the effective use of **AI-based Unsolicited Commercial Communication (UCC)** detection systems, specific rules and logics must be developed to ensure accurate identification, detection, and prevention of spam. These systems need to be robust, adaptive, and able to evolve with changing spam tactics. The following rules and logics are essential for training AI models and ensuring their success in combating spam:

1. Data Collection and Preprocessing Rules

- **Comprehensive Data Collection:**
 - Collect a broad dataset consisting of legitimate and spam communications (both calls and messages) to train AI models. This data should include various formats of spam, including promotional messages, phishing attempts, robocalls, etc.
- **Data Labelling:**
 - Manually label data as "spam" or "non-spam" (and possibly classify different types of spam), so the model can differentiate patterns. Accurate labelling is crucial for the model to learn correct patterns.
- **Feature Extraction:**
 - Identify key features from communication data, such as:

- Frequency of the communication from a sender.
 - Similarity of message content (repetitive keywords, phrases, URLs).
 - Timing patterns (e.g., repeated attempts within short time intervals).
 - Metadata such as sender ID, call duration, etc.
- **Natural Language Processing (NLP) Preprocessing:**
 - Normalize and preprocess text from SMS or call transcripts by:
 - Removing stop words, punctuation, and special characters.
 - Applying tokenization (breaking text into smaller parts) and stemming/lemmatization (reducing words to their root forms).
 - Vectorizing the text using algorithms like TF-IDF (Term Frequency-Inverse Document Frequency) to quantify the relevance of words.

2. Training AI Models

- **Supervised Learning:**
 - Use supervised learning techniques with labeled datasets to train the AI model to recognize spam patterns. Algorithms like **Random Forest**, **Support Vector Machines (SVM)**, or **Neural Networks** can be applied to classify communication as spam or non-spam.
- **Unsupervised Learning:**
 - Incorporate unsupervised learning techniques to detect new and emerging spam patterns. Clustering algorithms like **K-means** or **Autoencoders** can help detect unusual patterns in

communication behaviour that deviate from typical messages or calls.

- **Reinforcement Learning:**

- Use reinforcement learning to allow the AI model to learn from feedback over time. For example, if a communication is flagged as spam but later verified as legitimate, the model can learn from this mistake and adjust future decisions.

- **Adaptive Learning:**

- Implement continuous learning so that the model updates its knowledge as new types of spam emerge. The model should adapt based on new data and feedback.

3. Detection and Identification Rules

- **Content-Based Detection:**

- Train models to detect specific patterns in the content of messages or calls, such as:
 - **Keywords/phrases:** Repeated use of certain promotional phrases, offers, or deceptive terms (e.g., "free", "urgent", "act now").
 - **URLs:** Detection of suspicious or malicious URLs commonly used in phishing scams.
 - **Semantic Analysis:** Using NLP to understand the intent and meaning of the message, looking for signals of fraud or promotion.

- **Behavior-Based Detection:**

- Focus on the behaviour of the sender or caller rather than just the content. This includes:

- **Message frequency:** Flagging numbers that send multiple messages in a short period to different recipients.
- **Call frequency:** Detecting robocalls by analyzing the rate of calls made per minute.
- **Recipient diversity:** Monitoring whether a large number of messages are being sent to recipients from the same number.
- **Reputation scoring:** Assign a reputation score to a sender based on historical data (e.g., if a number has been flagged for spam in the past).
- **Anomaly Detection:**
 - Use AI models trained on normal user behaviour to detect anomalies. Anomalous behaviour could signal new or sophisticated spam attempts:
 - **Outliers in message structure:** Detect if a message deviates significantly from normal language patterns.
 - **Unusual sending times:** Spam campaigns may often occur during off-hours.
 - **Caller/Sender ID spoofing:** Detect patterns of caller ID manipulation that deviate from typical behaviour.

4. Prevention and Action Rules

- **Real-Time Detection and Blocking:**
 - Implement real-time detection mechanisms that can automatically flag or block suspicious messages or calls. This can be based on thresholds such as:

- Content similarity: If a message is sent repeatedly to different users with minimal variation.
- Blacklisted numbers: Automatically block communication from numbers previously flagged for spamming.
- **Feedback Loops:**
 - Create a feedback system where users can report incorrectly flagged messages (false positives) or missed spam (false negatives). The model should learn from this feedback to improve detection accuracy.
- **Multi-Layered Detection:**
 - Implement multiple layers of detection (e.g., combining content-based detection with behaviour-based analysis) to create a more comprehensive spam prevention system. This reduces false positives and enhances overall detection.

5. False Positive Reduction

- **Threshold-Based Detection:**
 - Define thresholds for flagging messages as spam based on multiple factors (content score, behaviour score, etc.). Fine-tune these thresholds to balance sensitivity and specificity, minimizing the chance of false positives.
- **Cross-Verification with Blacklists/Whitelists:**
 - Before flagging a message or call, cross-check the sender's number against known spammer blacklists and legitimate sender whitelists.
- **Sender Classification:**

- Use sender identification algorithms to classify the sender as a known entity (business, government, personal user, etc.). Messages from verified sources should be less likely to be flagged as spam unless strong indicators of spam are present.

6. Model Testing and Evaluation

- **Model Accuracy and Precision Metrics:**
 - Measure the performance of the AI model using metrics such as accuracy, precision, recall, and F1 score. This helps evaluate how well the model is detecting spam and avoiding false positives.
- **Regular Testing with Updated Data:**
 - Continuously test the model on newly collected data (both spam and legitimate communication) to ensure that it remains effective as spam tactics evolve.

7. Post-Detection Rules

- **Blacklist and Reputation Management:**
 - Automatically add flagged numbers to a dynamic blacklist, which can be shared across telecom service providers and authorities to prevent further spamming.
- **User-Driven Actions:**
 - Provide users with the ability to whitelist or blacklist senders at their discretion and integrate these user-driven actions into the model's learning process.
- **Regulatory Compliance:**

- Ensure that the detection system complies with TRAI's TCCCPR 2018 regulations regarding spam identification, reporting, and prevention measures.

8. Continuous Model Training and Updates

- **Continuous Learning Pipeline:**

- Set up a pipeline for continuous model training with fresh data to keep the model updated with the latest spam trends. This ensures that new types of spam or novel communication methods are detected.

- **AI Explainability:**

- Implement rules for AI model interpretability, so decision-making processes (why a message or call was flagged as spam) can be explained to users or auditors, ensuring transparency and accountability.

9. Integration with Telecom Service Providers

- **API Integration with Telecom Networks:**

- AI models should be integrated with telecom providers through APIs to enable real-time actions (e.g., blocking, filtering, reporting) at the network level, ensuring seamless spam prevention across all communication channels.

- **Collaborative Learning:**

- Telecom service providers can provide anonymized data on spam complaints to enhance the AI system's learning capabilities.

By applying these rules and logics, AI-based UCC detection systems can be highly effective in identifying, detecting, and preventing spam. Continuous learning and adaptation are crucial to keep the system responsive to evolving spam strategies.

b. Proactive actions needed to stop further communications of messages or calls identified as spam through UCC detect systems and actions on the senders.

Comments :

To stop further communications of messages or calls identified as spam through Unsolicited Commercial Communication (UCC) detection systems, proactive actions typically include the following measures:

1. Blocking the Sender's Access

- **Immediate Suspension of Sender IDs:** Upon detection of spam or UCC violations, sender IDs associated with the spam should be immediately blocked.
- **Revoking Short Codes:** Short codes used by spammers should be deactivated.
- **Blocking Bulk SMS Platforms:** Access to bulk SMS platforms used by the spammers should be disabled to prevent further messages.

2. Real-time Monitoring and Flagging

- **AI-Based Monitoring Systems:** Automated real-time detection systems should continuously monitor call and message traffic, identifying unusual patterns (such as high-frequency sending) and flagging them instantly for review.

- **Dynamic Blacklisting:** Create dynamic blacklists to automatically block senders based on repeat offenses or suspicious activities.

3. User Reporting Systems

- **Instant Reporting Channels:** Establish easy-to-use channels (e.g., toll-free numbers, apps, or SMS short codes) where recipients can report unwanted or spam messages/calls.
- **Feedback Loop:** Implement a system where user reports feed into the detection systems for faster and more accurate blocking of spammers.

4. Stricter Enforcement by TRAI

- **Action on Registered Telemarketers (RTMs):** If spam is sent through registered entities, regulatory bodies like the Telecom Regulatory Authority of India (TRAI) can revoke their registration, issue penalties, or take legal action.
- **Blocking Unregistered Telemarketers:** Detect and immediately block numbers or entities operating without registration and ensure enforcement actions against repeat violators.

5. Verification Mechanisms

- **Do Not Disturb (DND) List Compliance:** Ensure proactive checks against the DND registry so that users who have opted out do not receive unsolicited messages or calls.
- **Template Approval Systems:** Implement stricter checks and balances for message templates submitted by businesses to prevent the misuse of service templates for promotional content.

6. Penalizing Offenders

- **Heavy Fines and Legal Action:** Enforcement of financial penalties and legal action against habitual offenders can act as a deterrent for spammers.
- **License Revocation:** In cases of repeated violations, the service providers or telemarketers' licenses should be revoked.

7. Educating Consumers

- **Awareness Campaigns:** Launch campaigns to inform consumers about how they can identify spam and report it.
- **Promote DND Registration:** Encourage users to register their numbers on the DND list if they are frequently targeted by spammers.

These proactive measures can help ensure that once spam or UCC is detected, further communication is prevented, and the sender is appropriately penalized.

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 :

No comments.

b. Financial disincentive proposed in Section F of Chapter II on the access providers against violations in respect of UTM's

No Comments.

- c. **Financial disincentive against wrong approval of Headers and Message Templates proposed in Section F of Chapter II on the Access Providers.**

No Comments.

- 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.**

Comments :

To assign responsibilities to **Telemarketers** (both **Registered Telemarketers (RTMs)** and **Unregistered Telemarketers (UTMs)**) and **Principal Entities (Senders)** involved in sending Unsolicited Commercial Communication (UCC), regulatory frameworks need clear guidelines and enforcement measures. The following measures can be implemented to establish accountability, disincentivize spam, and ensure adherence to legal standards:

1. Clearly Defining Responsibilities

- **RTMs and UTMs:**
 - **Obligation to Register:** RTMs must comply with registration requirements, while UTMs need to be penalized for operating without registration.
 - **Adherence to Regulations:** RTMs are obligated to follow rules on sending messages and calls, maintaining a log of communications, and complying with UCC guidelines like template approval.
- **Principal Entities (Senders):**

- **Verification of Telemarketers:** Principal entities should ensure they engage only with registered and compliant RTMs.
- **Template Approval and Content Responsibility:** Principal entities are responsible for ensuring that content sent through RTMs adheres to regulatory standards and approved templates.
- **DND Compliance:** Both telemarketers and principal entities must ensure compliance with the Do Not Disturb (DND) registry and avoid sending promotional messages to DND-listed numbers.

2. Financial Disincentives

- **Fines for Violations:**
 - **RTMs and UTMs:** Heavy fines for violations like sending UCC to DND subscribers, non-compliance with template approval, and sending unsolicited messages can be imposed on both RTMs and UTMs.
 - **Principal Entities:** Entities found to be sponsoring or allowing UCC violations can also face substantial fines, ensuring shared responsibility.
- **Penalty Escalation for Repeat Offenses:** Repeat offenders, both telemarketers and senders, should face escalating financial penalties, which can deter future violations.
- **Service Disruption Fees:** When UCC is detected, a financial penalty could include a temporary suspension of services or higher operational costs for non-compliant entities.
- **Refunds to Consumers:** In cases of fraud or persistent harassment, consumers may be compensated by the telemarketer or principal entity.

3. Enforcement of Legal Actions

- **Telecom Regulatory Authority of India (TRAI) Enforcement:**
 - **Legal Penalties:** Under provisions of the Telecom Commercial Communication Customer Preference Regulations (TCCCPR), legal actions can be initiated against both RTMs and UTM, which can include court cases for substantial offenses.
 - **License Cancellation or Suspension:** RTMs that repeatedly violate regulations can face suspension or cancellation of their telemarketer licenses.
 - **Blacklist for UTM:** Unregistered telemarketers must be permanently blacklisted from telecom services for violating UCC regulations.
 - **Public Disclosure:** Publishing names of RTMs and senders involved in UCC violations can act as a deterrent.
- **Principal Entity Accountability:**
 - **Legal Responsibility for Content:** Principal entities should face legal action if they use unregistered telemarketers or send unsolicited promotional content, which can include criminal charges in cases of fraud.
 - **Contractual Obligations:** Contracts between principal entities and RTMs should include clauses mandating compliance with TRAI regulations, making entities liable for legal consequences if their telemarketers violate the rules.

4. Auditing and Monitoring

- **RTM and Principal Entity Audits:** Regular audits of telemarketers and principal entities should be conducted to verify their compliance with UCC laws. Non-compliant entities should face sanctions.
- **Data Retention and Reporting:** Both RTMs and principal entities should be required to maintain detailed records of communications (logs, templates, etc.) for a specified period. Failure to retain data should result in penalties.

5. Enhanced Consumer Protection

- **Simplified Reporting Mechanisms:** Ensure consumers have easy access to report UCC violations. Their complaints should trigger direct action against the responsible RTM or principal entity.
- **Consumer Rights to Compensation:** Strengthen legal frameworks allowing consumers to seek compensation for undue harassment through repeated UCC messages or calls.

6. Escalation Framework for UCC Violations

- **Progressive Sanctions:**
 - **First-Time Offenders:** Issue warnings and moderate fines for first-time offenders.
 - **Repeat Offenders:** Implement heavier fines, legal actions, and suspension or revocation of licenses.
 - **Habitual Offenders:** Imposing permanent blacklisting, legal actions, and severe fines against habitual violators.

7. Technology Solutions for Fraud Prevention

- **UCC Detection Systems:** Encourage RTMs and principal entities to invest in advanced technologies for UCC detection, ensuring they are more proactive in preventing unsolicited communication.
- **Template Verification:** Automated systems for template verification should be required to ensure messages conform to approved content categories.

These measures help ensure the responsible behavior of both telemarketers and principal entities and protect consumers from UCC while creating a regulatory and legal framework that holds violators accountable.

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?

Comments : **No.**

This is important for **maintaining affordability, distinguishing transactional from commercial content, and the societal benefits of reduced costs for essential communications.**

1. Transactional Messages Serve Essential Functions

- **Critical Information Delivery:** Transactional messages typically deliver important information like bank alerts, OTPs, flight notifications, or healthcare updates. These are essential services that consumers rely on for security and time-sensitive actions.

- **Customer Security and Fraud Prevention:** Many transactional messages, such as OTPs for two-factor authentication, play a crucial role in securing financial transactions and preventing fraud. Increasing costs could deter businesses from sending such important updates promptly.

2. Transactional Messages Are Non-Promotional

- **Different Purpose:** Unlike commercial messages, which aim to promote products or services, transactional messages provide information directly related to a customer's existing relationship with a company. Charging them at the same rate as promotional messages might not be justified, given their purely informative nature.
- **Maintaining Cost Efficiency:** Keeping the exemption recognizes the functional difference between transactional and promotional content. Since transactional messages are not designed to generate profit or sales, raising costs for them may be seen as unfair.

3. Increased Costs for Consumers and Businesses

- **Business Cost Burden:** Increasing the five-paisa exemption for transactional messages could significantly increase costs for businesses, particularly those in sectors like banking, healthcare, and logistics, where frequent transactional communication is required. These costs could be passed on to consumers.
- **Impact on Small Businesses:** Small and medium-sized businesses that rely on transactional messages to communicate with customers may find higher messaging fees prohibitive. This could limit their ability to provide timely notifications, thus affecting service quality.

4. Encourages Digital Financial Inclusion

- **Affordability for Financial Services:** In developing markets, especially where digital financial inclusion is being promoted, transactional messages (such as mobile banking updates or micro-loan reminders) serve as critical communication tools. Maintaining low costs for these messages supports greater access to financial services, especially for low-income individuals.
- **Supports Government Initiatives:** Many government schemes and services (such as COVID-19 vaccination alerts, social welfare notifications, etc.) rely on transactional messages. Keeping these affordable helps governments reach large populations with crucial updates without incurring high communication costs.

5. No Significant Revenue Impact for Telecom Operators

- **Minimal Revenue from Transactional Messages:** Transactional messages often constitute a small portion of overall telecom traffic, compared to bulk promotional messages. Therefore, the revenue potential from charging these messages at commercial rates might not be significant for telecom operators.
- **Preventing Overload on Promotional Channels:** If transactional messages are charged at commercial rates, businesses might seek alternative communication methods (like emails or app notifications) to avoid higher costs, which could reduce overall SMS traffic for telecom operators.

6. Supports a Clear Distinction Between Message Types

- **Prevents Misclassification of Messages:** Keeping the five-paisa exemption helps preserve a clear distinction between transactional and commercial messages. If both are priced the same, there could be confusion or misclassification of essential service-related communication as promotional.
- **Regulatory Simplicity:** Maintaining separate pricing structures for transactional and commercial messages allows for simpler enforcement and monitoring, making it easier for businesses to comply with message categorization guidelines.

7. Technological Costs and Infrastructure Management

- **Efficient Management of High-Volume, Low-Cost Traffic:** Many industries depend on the ability to send high volumes of transactional messages at low cost. Removing the exemption would impose additional costs on infrastructure management, especially in sectors like banking, where transaction confirmations are routine.
- **Encourages Use of Digital Channels:** By keeping transactional messages cost-effective, companies are encouraged to adopt digital communication channels, which can drive digital transformation and improved customer experiences.

Conclusion

The five-paisa exemption for transactional messages helps preserve the affordability of essential, non-promotional communications. It supports critical services like financial security, digital inclusion, and public service delivery, without adding an unnecessary financial burden on businesses or consumers. Therefore, maintaining this exemption ensures that businesses

can continue providing important updates to their customers in an efficient, cost-effective manner.

what additional measures are required to discourage senders, telemarketers or service providers from using transactional message templates for sending promotional messages?

To effectively discourage senders, telemarketers, and service providers from misusing **transactional message templates** for sending **promotional messages**, additional regulatory, technological, and enforcement measures are required. Here are key actions that can be taken:

1. Stricter Verification of Message Templates

- **Pre-Approval Process for Templates:** All message templates should go through a stricter approval process. This includes detailed scrutiny of the content to ensure it aligns with the transactional message category and doesn't contain any promotional material.
- **Regular Audits of Template Use:** Regulatory bodies should conduct random audits on the use of pre-approved transactional message templates by senders and telemarketers. These audits can help identify whether any promotional messages are being sent under transactional templates.

2. AI-Based Content Filtering

- **AI and Machine Learning Tools:** Telecom operators and regulatory bodies can implement AI-driven content filtering systems to analyze message content in real time. These tools can automatically flag content that appears promotional, even if sent using transactional templates.

- **Natural Language Processing (NLP):** Advanced NLP models can detect promotional keywords or phrases and cross-check them against the pre-approved purpose of the transactional template. If detected, the system can halt message transmission.

3. Penalties and Financial Disincentives

- **Hefty Fines for Violations:** Enforce significant financial penalties for senders and telemarketers found misusing transactional templates for promotional messages. The fines should be large enough to serve as a deterrent, especially for repeated violations.
- **Escalating Penalties for Repeat Offenders:** Implement a tiered penalty system where penalties increase for repeat violations, and ultimately, service access can be suspended for chronic offenders.
- **Compensation to Consumers:** Introduce compensation mechanisms for consumers who receive unsolicited promotional messages under transactional routes, further disincentivizing misuse.

4. Blacklisting and Blocking Offenders

- **Blocking Access for Offenders:** Telemarketers or senders who are repeatedly caught sending promotional messages using transactional templates should have their access to transactional message services suspended or terminated.
- **Permanent Blacklisting:** For habitual offenders, implement permanent blacklisting from sending any transactional or promotional messages across networks. Their registration or licenses could also be revoked.

5. Mandatory Logging and Reporting

- **Message Delivery Logs:** Mandate that service providers maintain detailed logs of all messages sent, including message templates, content, and classification (transactional or promotional). This data can be subject to regular inspections by regulators.
- **Transparent Reporting to Regulators:** Telemarketers and senders should be required to report their usage of transactional templates on a periodic basis. Any discrepancies or signs of misuse can then trigger investigations.

6. Consumer Reporting and Feedback Mechanism

- **Easy Consumer Reporting Channels:** Establish simple, accessible channels (such as toll-free numbers or apps) for consumers to report receiving promotional messages disguised as transactional. Complaints should be investigated promptly and trigger action.
- **Incentivized Consumer Reports:** Consider rewarding consumers for reporting misuse, such as providing small incentives, which can increase the detection of violations.

7. Clear Definition of Transactional and Promotional Categories

- **Reinforcing Regulatory Definitions:** Strengthen the distinction between transactional and promotional messages by providing clearer regulatory guidelines and educating businesses about what constitutes each type of message.
- **Regular Training for Telemarketers and Businesses:** Conduct training sessions for businesses and telemarketers to help them understand the consequences of template misuse and ensure compliance with messaging rules.

8. Segregation of Messaging Platforms

- **Dedicated Channels for Promotional Content:** Encourage or mandate the use of separate communication channels or short codes for promotional and transactional content. This helps maintain clarity and prevents the mixing of the two categories.
- **Service Provider Oversight:** Require service providers to segregate their traffic for different types of messages and monitor the use of transactional routes. Providers should also be penalized if they allow the mixing of promotional messages through transactional channels.

9. Use of Digital Signatures for Templates

- **Digital Signature Verification:** Introduce a system where each approved template (whether transactional or promotional) must have a unique digital signature. This would make it easy to track whether the right templates are being used for the intended purpose.
- **Automated Compliance Checks:** Develop an automated compliance system that checks each message for template conformity and disallows messages that fail the checks from being sent.

10. Limiting the Frequency of Transactional Messages

- **Frequency Caps on Transactional Messaging:** Implement frequency limits for transactional messages to ensure that companies do not misuse these messages by over-sending them as a promotional tactic. For example, limiting the number of daily or weekly transactional messages per user.

11. Service Provider Liability

- **Holding Providers Accountable:** Make telecom operators and service providers accountable for ensuring that transactional routes are not used for promotional purposes. Providers should be penalized if they allow violators to misuse their platforms.
- **Joint Responsibility of Senders and Providers:** Both the sender (principal entity) and the telecom provider/telemarketer should share responsibility for ensuring compliance with messaging rules.

These additional measures focus on strengthening **content monitoring, increasing penalties,** and ensuring **regulatory oversight,** which can effectively discourage the misuse of transactional templates for sending promotional messages. Combining technological solutions like AI with stronger enforcement and reporting mechanisms can create a robust deterrent for violators.

Q.11 Stakeholders are requested to offer their comments on the following issues:

- 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?**

Comments : **Yes.**

Yes, there is a clear need to strengthen the provisions of the **Common Code of Practice** templates, along with **Standard Operating Processes (SOPs),** to empower **Access Providers** to take more decisive actions,

including imposing **financial disincentives** and legal actions, against entities that are registered but fail to follow regulations. The following points highlight the rationale for strengthening these provisions:

1. Increasing Accountability of Registered Entities

- **Compliance Enforcement:** Registered telemarketers and entities are required to adhere to specific guidelines and regulations under the **Telecom Commercial Communication Customer Preference Regulations (TCCCPR)**. However, many entities find loopholes or exploit the system by sending unsolicited commercial communication (UCC). Strengthening the Common Code of Practice templates with clear SOPs will ensure stricter compliance and accountability.
- **Detailed SOPs for Monitoring:** Stronger, more detailed **Standard Operating Processes** will provide access providers with the necessary tools to monitor the adherence of registered entities to messaging rules. These SOPs could include real-time tracking of message content, categorization, and compliance with approved templates.

2. Effective Financial Disincentives

- **Escalating Financial Penalties:** The current financial disincentives may not be sufficient to discourage entities from violating the guidelines. By enhancing the provisions, financial penalties can be scaled up significantly for repeat offenders, making it economically unsustainable for businesses to violate the regulations.
- **Direct Impact on Revenue:** Imposing higher financial disincentives will act as a more potent deterrent for entities that misuse messaging

templates or flout regulations. The threat of substantial financial loss can encourage compliance and responsible use of communication channels.

3. Clearer Framework for Actions Against Violations

- **Automated Enforcement Mechanisms:** Access providers need a clear and standardized framework that automates actions like suspending services, issuing warnings, or imposing financial disincentives when violations are detected. These provisions will reduce the time lag in taking action against violators and ensure a more proactive approach to enforcement.
- **Triggering Legal Actions for Persistent Violators:** Strengthening the SOPs will allow access providers to initiate legal proceedings against habitual violators, whether they are registered or unregistered. Such provisions ensure that non-compliance is met with serious consequences, including criminal liability if necessary.

4. Improved Detection and Prevention of UCC Violations

- **Enhanced Monitoring Capabilities:** By updating the Common Code of Practice templates, access providers can deploy better monitoring mechanisms that allow real-time analysis of message content and the intent behind the communication. This will help detect promotional content being sent under transactional message categories or unauthorized use of templates.
- **Improved Fraud Detection:** Strengthened SOPs will allow for the development of sophisticated fraud detection systems that can quickly identify and block fraudulent telemarketers or unregistered entities engaging in unsolicited communications.

5. Disincentivizing Unregistered Entities

- **Targeting Unregistered Entities (UTMs):** Unregistered telemarketers (UTMs) who bypass the system often operate outside the regulatory framework. Strengthening the provisions would give access providers the authority to take immediate action against UTMs, including financial disincentives and legal measures. This can reduce the number of unsolicited communications coming from these rogue entities.
- **Blocking Telecom Services to UTMs:** Strengthened provisions should enable access providers to block or suspend telecom services for unregistered entities and those that are persistently non-compliant. This adds a layer of enforcement that can cut off UCC at its source.

6. Transparency and Consumer Protection

- **Clearer Guidelines for Consumers:** Strengthening the Common Code of Practice will also provide clarity to consumers on what constitutes a violation and how they can report it. Ensuring that consumers have a clear process to report unsolicited communications will increase transparency and accountability.
- **Provisions for Compensation:** Consider introducing consumer compensation provisions, where businesses that violate UCC regulations by sending unsolicited messages or misusing templates are required to compensate affected consumers. This further disincentivizes non-compliance.

7. Empowering Access Providers for Immediate Action

- **Authority to Impose Penalties Directly:** Empowering access providers to take immediate and autonomous action, including imposing penalties without waiting for a regulatory directive, will make enforcement more efficient. This would streamline the process and ensure that violators are penalized as soon as they are identified.
- **Suspension of Services:** Strengthened provisions would allow access providers to temporarily or permanently suspend services for entities that fail to follow regulations, without requiring additional regulatory approvals. This swift action can serve as a strong deterrent.

8. Enhancing the Role of the Regulator

- **Regulatory Oversight and Reporting:** Strengthening the provisions should include regular reporting mechanisms where access providers submit compliance reports to the regulator. This ensures that actions taken are consistent with regulatory goals and that violators are dealt with uniformly.
- **Collaboration Between Telecom Operators and Regulatory Bodies:** Telecom operators and regulators must work together to ensure that disincentives are applied consistently, and habitual violators are flagged across the system to prevent repeat offenses.

9. Adapting to Changing Technological Landscapes

- **Addressing New Communication Channels:** As communication technologies evolve (e.g., WhatsApp Business, RCS messaging, etc.), the provisions need to be flexible enough to cover these new platforms. This ensures that access providers can take action regardless of the communication medium being misused.

- **Continuous Review of Regulations:** There should be a built-in mechanism for continuous review and updating of the Common Code of Practice templates and SOPs to keep up with emerging technologies and communication trends, ensuring that loopholes are closed promptly.

In short, Strengthening the provisions of the Common Code of Practice templates with Standard Operating Processes is necessary to give access providers more tools to take decisive action against non-compliant entities. By enhancing enforcement capabilities, introducing financial disincentives, and clarifying legal consequences, the regulatory framework will better protect consumers, ensure compliance, and significantly reduce unsolicited commercial communication.

Additional Provision and Essential Process :

1. Enhanced Monitoring and Auditing:

- **Regular Audits:** Ensure that Access Providers conduct regular audits of registered entities to verify compliance with template usage regulations.
- **Real-time Monitoring:** Implement real-time monitoring systems for detecting misuse or non-compliance, such as sending unsolicited messages or using templates for purposes other than those registered.
- **Data Sharing:** Enable data sharing between Access Providers and relevant authorities for faster identification of violations.

2. Financial Disincentives and Penalties:

- **Graduated Penalty Structure:** Define a tiered system of financial penalties based on the severity and frequency of violations (e.g., higher fines for repeat offenders).
- **Instant Penalty Mechanism:** Introduce mechanisms for Access Providers to immediately impose financial disincentives for minor infractions, such as using incorrect or unregistered templates.
- **Escalating Fines for Recurring Offenses:** Increase fines for repeat violators to deter future non-compliance.

3. Standardized Reporting Mechanism:

- **Complaint Tracking:** Establish a standardized platform for reporting template misuse, with complaint tracking and resolution mechanisms for both consumers and Access Providers.
- **Whistleblower Provisions:** Encourage and protect internal reporting within organizations using the CoPs, with specific rewards or protections for reporting non-compliance.

4. Compliance Verification and SOPs:

- **Template Verification:** Introduce a system for verifying the use of templates before sending communication. This can include cross-checking the content, time, and purpose against registered template details.
- **Automated Alerts:** Develop SOPs for Access Providers to send automated alerts to registered entities when non-compliant behavior is detected, offering a grace period to rectify issues.
- **Random Inspections:** Conduct random inspections of registered entities' messaging and call systems to ensure compliance with regulations.

5. Legal Framework and Escalation:

- **Escalation of Non-compliance to Legal Authorities:** Set clear guidelines for when Access Providers must escalate severe non-compliance cases (e.g., fraud or deceptive practices) to legal authorities for action.
- **Binding Agreements:** Require entities to sign binding agreements when registering templates, ensuring they understand that violations could lead to legal proceedings.

6. Transparency and Accountability:

- **Public Disclosure of Violators:** Publish names of entities that have violated CoPs as a deterrent and to promote accountability.
- **Template Re-registration Requirement:** Force repeat offenders to re-register their templates and undergo a compliance review before being allowed to resume normal operations.

7. Education and Training:

- **Mandatory Training:** Require registered entities to complete periodic training on the use of templates and compliance with CoPs.
- **Public Awareness Campaigns:** Inform the public about how to report misuse and the steps taken by Access Providers to ensure compliance.

8. Consumer Protection and Redressal Mechanism:

- **Quick Redressal System for Consumers:** Implement a fast-track system for consumers to lodge complaints regarding misuse of registered templates, with clear timelines for resolution.

- **Financial Compensation for Consumers:** Offer provisions where consumers impacted by non-compliant messaging or calls can seek compensation.

These measures can help tighten regulatory compliance and promote a transparent, accountable system for managing promotional communication, benefiting both consumers and entities.

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 encashment/replenishment of security deposits against the breach of the regulations? Please provide your answers with suitable justifications.

Comments : **Yes.**

Introducing a **minimum security deposit** provision from entities registering with Access Providers could be an effective way to deter misuse or breach of regulations. This would create a financial incentive for entities to comply with the guidelines, as non-compliance could result in forfeiture or penalties deducted from their deposit. Here are key considerations for implementing such a provision:

1. Purpose of Security Deposit:

- **Deterrent for Misuse:** The security deposit acts as a safeguard against the misuse of messaging/calling templates or violations of regulations.

- **Compensation for Violations:** In case of non-compliance, a part of the security deposit can be used to cover fines, penalties, or even compensation to affected consumers.
- **Incentive for Compliance:** Entities are incentivized to follow regulations to avoid losing their deposit.

2. Deposit Amount Structure:

- **Tiered Deposit Based on Risk:** Set different security deposit amounts based on the scale of operations or the type of entity (e.g., higher for entities with larger volumes of communication or higher-risk industries).
- **Refundable on Compliance:** Ensure the deposit is refundable after a certain period of sustained compliance, or upon voluntary deregistration, provided no violations have occurred.

3. Provisions for Deduction and Forfeiture:

- **Automatic Deduction for Minor Violations:** Minor breaches (e.g., unauthorized template usage, unsolicited communication) could lead to automatic deductions from the deposit.
- **Forfeiture for Major Violations:** For serious breaches (e.g., fraud, repeated offenses, harmful messages), the entire deposit could be forfeited, and legal action pursued.
- **Escalating Deductions:** Implement a structure where repeated violations lead to progressively higher deductions, encouraging corrective behaviour early on.

4. Replenishment Requirement:

- **Mandatory Replenishment:** After any deduction, entities should be required to replenish the security deposit to maintain their registration status. Failure to do so could lead to suspension or deregistration.

5. Link to Volume of Communication:

- **Scaling with Communication Volume:** Larger entities or those sending high volumes of messages should provide a higher security deposit to account for the increased risk of misuse.

6. Holding Period:

- **Fixed Holding Period:** The deposit could be held for a minimum duration, such as the period of active registration, and released only after the Access Provider verifies compliance during and after the entity's operations.

7. Transparency in Enforcement:

- **Clear Terms for Use of Deposit:** Ensure that the terms and conditions regarding deductions or forfeiture from the deposit are transparent, and entities are clearly informed about the reasons for any action taken.
- **Appeal Mechanism:** Provide an appeal process for entities to challenge deductions they believe are unjustified.

8. Industry-Specific Flexibility:

- **Different Security Levels for Different Sectors:** The security deposit amount could vary depending on the sector, with high-risk sectors (e.g., financial services, insurance, marketing) requiring higher deposits due to the increased likelihood of misuse.

9. Inclusion in Regulatory Framework:

- **Incorporate into CoPs:** This provision can be part of the Common Code of Practice (CoPs) for Access Providers, ensuring uniformity across the industry and making it a standard requirement for all entities.

10. Insurance-Based Alternative:

- **Option for Insurance Coverage:** Entities could be allowed to provide proof of compliance insurance as an alternative to a direct security deposit, with the insurance covering any penalties or damages.

Benefits of Security Deposit Provision:

- **Accountability:** Entities would be more cautious in their operations, knowing that misuse could lead to financial losses.
- **Consumer Protection:** Ensures there is a financial mechanism to compensate consumers or regulatory bodies for any harm caused by non-compliance.
- **Reduced Regulatory Burden:** Reduces the need for heavy monitoring, as entities would self-regulate to avoid penalties.

By implementing a security deposit system, Access Providers can further strengthen the enforcement of regulations and ensure that entities adhere to the required standards, fostering a more responsible communication ecosystem.

Encashment/Replenishment of Security Deposits :

The **encashment/replenishment** of security deposits in case of a breach of regulations by entities registering with Access Providers should

follow a well-defined, transparent, and fair process. This ensures that the system effectively deters misuse while allowing entities to maintain their operations by replenishing deposits when necessary.

Here's how the encashment and replenishment process could be structured:

1. Encashment Process for Security Deposit:

a. Clear Identification of Breach:

- Access Providers must have a transparent system for identifying breaches of regulations, such as misuse of messaging templates, unsolicited communication, or other violations.
- Automated systems and audits can be used to flag non-compliance, ensuring there is sufficient evidence before triggering the encashment process.

b. Notification of Breach:

- **Immediate Notification:** Upon detecting a breach, the Access Provider should notify the entity of the violation in writing, specifying the nature of the breach, the corresponding regulatory provision, and the proposed penalty amount to be deducted from the security deposit.
- **Grace Period:** Provide a short grace period (e.g., 5-10 business days) for the entity to dispute or rectify the breach before the encashment of the deposit.

c. Proportional Encashment:

- **Proportional to Severity:** The amount deducted from the security deposit should be proportional to the severity of the breach. For example:
 - **Minor Infractions:** Small deductions for first-time or minor violations (e.g., unauthorized use of templates).
 - **Major Infractions:** Higher deductions for serious violations (e.g., fraudulent communication, repeat offenses).
- **Cumulative Penalty System:** Implement a cumulative penalty system where repeat breaches result in higher encashment amounts.

d. Escalation for Non-compliance:

- For entities that continue to breach regulations without rectification, **partial or full forfeiture** of the deposit should be considered, along with possible suspension or deregistration.
- **Legal Action:** In cases of severe non-compliance, legal action may be taken beyond the encashment of the deposit.

2. Replenishment Process of Security Deposit:

a. Replenishment Notification:

- After encashment of any part of the deposit, Access Providers should immediately notify the entity to **replenish the deposit** back to the original level within a stipulated time (e.g., 30 days).
- Include detailed information on the amount deducted and the reason, as well as instructions for how and when to replenish the deposit.

b. Suspension for Failure to Replenish:

- **Suspension of Services:** If the entity fails to replenish the deposit within the required time frame, the Access Provider should suspend the entity's ability to send further communications until the deposit is fully restored.
- **Temporary Suspension:** A temporary suspension of registration status can be applied if the deposit is not replenished within the stipulated period. After a set period (e.g., 60 days), if the deposit is still not replenished, a more permanent suspension or deregistration may follow.

c. Automatic Replenishment Option:

- **Pre-authorized Debit System:** Offer entities the option to set up a pre-authorized debit system, where their account is automatically charged to replenish the deposit once deductions are made. This ensures minimal disruption to their operations.

d. Flexible Replenishment Based on Risk Profile:

- Entities with a history of compliance could be given **longer replenishment periods** or allowed to partially replenish their deposits over time.
- For high-risk entities or repeat offenders, a more stringent replenishment schedule should apply (e.g., immediate replenishment required within 7 days).

3. Transparency and Documentation:

a. Transparent Encashment Process:

- Every encashment event should be **well-documented** with clear communication to the entity explaining the violation and the associated penalty.
- A record of all encashments, notifications, and replenishments should be maintained and made available to the entity upon request.

b. Right to Appeal:

- Provide the entity with an opportunity to **dispute the penalty** or encashment decision through an appeals process. This can include an internal review or submission of supporting evidence that the entity was compliant.
- If the appeal is successful, the deducted amount should be refunded back to the deposit.

4. Deposit Top-up Requirements:

a. Periodic Top-ups for Larger Entities:

- For entities that engage in **high-volume communications**, there could be a requirement to periodically top up their security deposit, especially if the volume or risk profile increases over time.
- Access Providers may reassess security deposit levels annually based on the entity's past behavior and current communication volume.

5. Encashment Escalation Based on Breach Frequency:

a. Incremental Penalty System:

- For each subsequent breach, the penalty deducted from the security deposit should **escalate** (e.g., a 10% deduction for the first breach, 20% for the second, etc.).
- Repeated non-compliance should result in full encashment and possible termination of the entity's registration.

6. Public Disclosure and Accountability:

- **Transparency to Stakeholders:** Access Providers should have provisions for **publicly disclosing** entities that repeatedly breach regulations or fail to replenish their security deposits.
- **Report to Regulatory Authorities:** If necessary, Access Providers should report chronic offenders to regulators for further action or enforcement beyond financial penalties.

7. Refund upon Deregistration:

- When an entity voluntarily deregisters or stops its communication services, the **remaining security deposit** should be refunded, provided that there are no outstanding penalties or breaches.
- A final audit should be conducted before refunding the deposit.

Benefits of This Approach:

- **Accountability and Deterrence:** This process creates financial accountability and dissuades entities from breaching regulations.
- **Operational Continuity:** Allowing replenishment ensures that entities can continue operations while rectifying non-compliance.
- **Fairness and Transparency:** A clear system for encashment and replenishment ensures fairness, with entities aware of the consequences and given opportunities to rectify breaches.

By implementing this encashment and replenishment structure, Access Providers can maintain a balance between regulatory enforcement and the operational flexibility of registered entities.

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

Comments :

Unsolicited Commercial Communication (UCC), including spam calls and messages, is a significant challenge for TRAI. Addressing this issue through tariff mechanisms is an innovative approach that can create financial disincentives for entities engaged in UCC while protecting consumers. Here are some **effective steps that can be taken through tariffs** to control UCC:

1. Premium Tariffs for Bulk Messaging and Calls:

- **Higher Tariffs for Commercial Communication:** Implement higher tariffs for sending bulk SMS or making bulk calls, especially for promotional and marketing purposes. Entities that send UCC would face higher costs, which would disincentivize mass unsolicited communication.
- **Differential Pricing for Registered vs. Unregistered Entities:** Introduce differential tariffs for entities registered with Access Providers for legitimate promotional communications. Registered entities can enjoy lower rates, while unregistered entities that send bulk communication face higher charges.

2. Per UCC Penalty-Based Tariff:

- **Per Message or Call Penalty:** Introduce a system where each UCC message or call that breaches regulations incurs a **penalty tariff**, automatically added to the sender's bill. This penalty could be progressively higher for repeat offenders, significantly raising the cost of non-compliance.
- **Automated Detection and Billing:** Utilize automated systems that detect UCC and apply penalties in real-time based on message/call characteristics, including sender type, message content, and recipient complaints.

3. Progressive Tariff for High-Volume Senders:

- **Tiered Tariff System for High-Volume Messaging/Calling:** Introduce progressive tariffs that increase based on the volume of promotional messages or calls made by an entity. This could include **higher rates after certain thresholds**, making it financially unviable for spammers to continue large-scale operations.
- **Discounted Tariffs for Compliance:** Entities that comply with regulations (such as registering templates or using Do Not Disturb (DND) lists) could receive **discounted bulk tariffs**, encouraging legitimate use of the network.

4. Tariff Penalties for Non-Compliant Entities:

- **Additional Surcharges for Non-Compliant Communications:** Introduce surcharges or increased tariffs for messages or calls sent by entities that fail to comply with **DND regulations** or misuse **telecom template codes**.
- **License-Based Tariffing:** Entities without the proper registration or licenses for sending promotional communications could be charged

a **significantly higher tariff**, creating an economic disincentive for violating UCC regulations.

5. Pre-Paid Credit Mechanism for Bulk Messaging:

- **Pre-Paid Messaging Accounts:** Require businesses to pre-pay for bulk messaging or calls, with strict oversight to ensure only compliant messages/calls are delivered. **Pre-paid credits could be forfeited** in cases of non-compliance with UCC regulations.
- **Deposit-based Bulk Messaging:** Entities must deposit a specific amount before sending bulk communications. This deposit could be linked to UCC compliance and is reduced if violations are detected.

6. Blacklist-Based Tariff Increases:

- **Higher Tariffs for Blacklisted Numbers:** Numbers or entities flagged for frequent UCC violations could face automatic increases in tariffs, significantly raising the cost of sending further communications.
- **Incremental Tariffs Based on Violations:** Introduce a **sliding scale of tariffs** that increases as the number of complaints against a sender rises, making it progressively more expensive for entities that engage in UCC.

7. Tariff Penalties for Multiple SIM Use:

- **Tariff Monitoring Across SIM Cards:** Implement stricter tariff policies for businesses or individuals using multiple SIM cards to circumvent UCC regulations. Higher tariffs could be imposed for entities or individuals suspected of using multiple SIMs to bypass bulk messaging caps.

- **Linked Tariff Structures for Bulk Message Senders:** Telecom providers could link tariffs to the number of SIMs used by an entity, with a progressive increase in costs for those using multiple SIMs for UCC purposes.

8. Tariffs Linked to Opt-Out Rates:

- **Penalty Tariffs for High Opt-Out Rates:** If an entity has a high rate of **DND or opt-out requests** from consumers, Access Providers could increase the tariffs for sending further messages or calls. This would create a direct financial consequence for sending unsolicited communications.
- **Progressive Increase for Repeat Opt-Out Offenses:** Entities that frequently violate opt-out requests (e.g., repeatedly contacting individuals who have opted out) could face progressively higher tariffs each time a violation occurs.

9. Tariffs Based on Complaint Ratios:

- **Complaint-Linked Tariff Adjustments:** Implement a system where tariffs are adjusted based on the ratio of complaints received about UCC from a particular sender. High complaint ratios could lead to **tariff hikes** for that sender.
- **Rebate for Low Complaint Rates:** Entities that maintain low complaint rates and comply with UCC regulations could be given **rebates** or discounts on their promotional messaging tariffs, rewarding good practices.

10. Separate Tariffs for Non-Promotional vs. Promotional Messages:

- **Differential Tariffs for Promotional Content:** Differentiate tariffs between **promotional** and **non-promotional** messages, with higher charges applied to promotional content. This will ensure that entities are more mindful about sending only necessary and compliant messages.
- **Template-Based Tariffing:** Charge higher tariffs for messages that don't follow registered templates, encouraging businesses to register and comply with approved communication formats.

11. Usage Caps with Financial Penalties:

- **Usage Caps for Promotional Communication:** Set strict caps on the number of promotional messages or calls that can be sent by any entity within a specific period (e.g., daily, weekly). Exceeding these limits would lead to **steep financial penalties or higher tariffs**.
- **Progressive Penalties for Cap Violations:** Apply progressive tariffs for entities that breach their usage caps, increasing the cost for each additional message or call sent beyond the limit.

12. Consumer-Focused Tariff Mechanisms:

- **Incentives for Opting into Promotional Messaging:** Offer consumers **tariff discounts or free services** if they opt into receiving promotional messages from legitimate businesses, thus creating a market for voluntary engagement rather than unsolicited UCC.
- **Financial Penalties for Breaching DND Preferences:** Introduce immediate financial penalties for entities that contact consumers on the **DND list**. These penalties could be charged directly to the sender's account.

13. Periodic Review and Adjustment of Tariffs:

- **Dynamic Tariff Adjustment:** Regularly review and adjust tariffs based on the effectiveness of the existing measures, ensuring that UCC-related tariffs remain sufficiently high to deter misuse while promoting compliant communication.

Benefits of Tariff-Based Measures:

- **Financial Disincentive:** These tariffs would create a direct financial cost for entities engaging in UCC, making it less profitable or cost-prohibitive for them to continue.
- **Encourages Compliance:** By offering lower tariffs for compliant behavior and higher tariffs for non-compliance, entities are incentivized to follow UCC regulations and use legitimate communication channels.
- **Consumer Protection:** Tariff measures protect consumers from receiving unsolicited messages and calls by creating a significant cost for entities engaging in UCC.
- **Revenue Generation for Enforcement:** The additional revenue generated through higher tariffs and penalties can be reinvested into better monitoring and enforcement systems for UCC.

By leveraging tariffs strategically, Access Providers can significantly curb the UCC menace while ensuring that businesses have the incentive to adhere to regulatory requirements.

Q.13 Whether differential tariff for SMS and Voice calls beyond a certain limit should be introduced to disincentivize UCC through UTM? Please justify.

Comments :

Yes, **differential tariffs for SMS and voice calls beyond a certain limit should be introduced to disincentivize Unsolicited Commercial Communication (UCC) through Unregistered Telemarketers (UTMs).** Here's why:

1. Financial Disincentive for UCC:

- **High-Volume Messaging and Calling:** UTMs frequently send large volumes of unsolicited messages and make unsolicited calls. Imposing a **differential tariff** beyond a certain limit would increase the cost for high-volume UCC, directly reducing the economic viability of such practices.
- **Costlier for Non-Compliant Entities:** Since UTMs typically bypass registration and regulatory oversight, applying higher tariffs would make it more expensive for them to operate. This would push them towards compliance or reduce their UCC activities.

2. Encouraging Legitimate Practices:

- **Motivates Registration:** Differential tariffs would encourage UTMs to register as legitimate telemarketers, as registered entities can enjoy lower rates. This would lead to better regulatory oversight and increased accountability.
- **Quality over Quantity:** The financial burden of higher tariffs would push marketers to focus on **targeted and high-quality communications**, rather than indiscriminate mass messaging or calling.

3. Consumer Protection:

- **Reducing Spam:** Differential tariffs beyond a threshold act as a cap on unsolicited communications, protecting consumers from being overwhelmed by spam messages and calls.
- **Respecting DND Preferences:** Higher tariffs would encourage businesses to respect **Do Not Disturb (DND)** preferences, as repeated violations would become too costly.

4. Creates a Fair System:

- **Balancing Usage and Costs:** Entities that adhere to regulations and use communication channels responsibly would not be disproportionately impacted. The tariffs would only rise after a reasonable limit, ensuring that legitimate communication isn't penalized while targeting excessive spamming.

5. Supports Enforcement:

- **Real-Time Monitoring:** Access Providers can use this tariff structure to track UCC patterns and flag potential misuse by UTM's. This provides better enforcement tools to control the spread of unsolicited communications.

In conclusion, **differential tariffs beyond a certain limit** would effectively reduce the volume of UCC by imposing higher costs on UTM's, thus incentivizing responsible communication and protecting consumers from unwanted contact.

Justification :

Introducing a **differential tariff for SMS and voice calls** beyond a certain limit for Unsolicited Commercial Communication (UCC) sent via

Unregistered Telemarketers (UTMs) can be an effective way to disincentivize UCC. Here's why such a measure should be considered and how it can be justified:

Justifications for Differential Tariffs for SMS and Voice Calls Beyond a Limit:

1. Direct Financial Disincentive for UCC:

- **Higher Costs for Excessive Usage:** UTMs often send high volumes of unsolicited messages and make calls in bulk, exploiting low-cost communication channels. Introducing a differential tariff beyond a certain limit would **increase the cost of sending mass UCC**, directly affecting the profitability of such activities.
- **Reduced Incentive for Spammers:** By escalating tariffs after a threshold, UTMs would face significant financial barriers to continuing mass unsolicited communications, thereby reducing their incentive to engage in spamming.

2. Targeting UTMs without Regulatory Compliance:

- **UTMs Bypass Regulations:** UTMs often bypass registration and regulatory requirements, making it difficult for authorities to track or control their activities. By introducing higher tariffs beyond a set limit, it becomes harder for UTMs to avoid scrutiny, and they would face penalties even if they are unregistered.
- **Encouraging Registration:** Differential tariffs would also encourage businesses to register as legitimate telemarketers. Registered telemarketers can be offered lower rates, while UTMs would face

progressively higher costs for excessive usage, motivating them to formalize their activities.

3. Capping UCC to Protect Consumers:

- **Consumer Protection from Spam:** UCC creates a significant burden on consumers, especially when sent in large quantities. A differential tariff would serve as an **upper limit or cap** on how many unsolicited messages or calls can be sent, protecting consumers from spam overload.
- **Threshold for Legitimate Communication:** The set limit for the number of messages or calls can be calibrated to allow **genuine business communication**, while excessive messaging beyond the limit would face punitive costs, targeting spam specifically.

4. Incentivizing Responsible Communication:

- **Encouraging Quality Over Quantity:** When UCCs know they will face higher tariffs beyond a certain threshold, they would focus on **targeted, high-quality communication** rather than blasting mass UCC indiscriminately. This promotes a more responsible and efficient use of communication channels.
- **Better Compliance with Opt-Out and DND Preferences:** Facing higher tariffs, UCCs would have an incentive to respect opt-out requests and Do Not Disturb (DND) lists, as repeated UCC violations would become financially unsustainable.

5. Scalable to Different Business Models:

- **Fair for Small and Large Businesses:** The limit for differential tariffs could be set high enough so that **small businesses** or legitimate

users sending occasional marketing messages are not unduly affected. Large-scale operations, typical of UCC, would be the ones primarily impacted.

- **Targeting High-Volume Spammers:** By scaling the tariffs progressively, high-volume spammers would face significantly higher costs, while entities with low or moderate messaging volumes would not be disproportionately affected.

6. Enhances Monitoring and Detection:

- **Flagging Potential Abuse:** If a UTM exceeds the pre-set limit for sending SMS or making voice calls, this can trigger **automated flags** for the Access Provider or regulatory authority to investigate the entity further. Differential tariffs can be used as an indicator of potential abuse of communication channels.
- **Data Collection for Enforcement:** The system of differential tariffs would also help in data collection, allowing authorities to **track trends and behaviors** of potential spammers, enabling better enforcement.

7. Aligns with "Polluter Pays" Principle:

- **Higher Tariffs for Higher UCC Load:** UTMs that send excessive UCC create a higher burden on telecom networks and regulatory resources. By introducing differential tariffs, the "polluter pays" principle is applied, where those creating more unsolicited communication bear a proportionally higher cost, helping to **offset the regulatory and network management costs.**

8. Revenue Generation for Better UCC Management:

- **Fund Enforcement and Consumer Awareness:** The additional revenue generated from higher tariffs can be used by Access Providers and regulators to fund **UCC monitoring systems, complaint redressal mechanisms, and consumer awareness programs**. This revenue can also support better compliance monitoring for registered telemarketers.

Implementation Considerations:

1. Threshold Setting:

- **Determine a Reasonable Limit:** The threshold for differential tariffs should be set based on industry norms, allowing sufficient room for legitimate communication while targeting mass UCC. For example, a business might be allowed to send 1000 messages/calls at a standard rate, with tariffs increasing for every 1000 messages/calls thereafter.

2. Progressive Tariff Structure:

- **Increasing Tariffs for Higher Volumes:** A progressively increasing tariff structure ensures that UTMs face higher costs as they increase the volume of UCC. This could be done through tiers (e.g., up to 1000 messages at the base rate, the next 1000 at 1.5x, and so on).

3. Penalties for Violations:

- **Link to Regulatory Violations:** Tariff increases could also be tied to specific regulatory violations, such as contacting users on DND lists, sending unauthorized templates, or exceeding limits without proper authorization.

4. Encouraging Legitimate Use:

- **Lower Rates for Registered Telemarketers:** To encourage compliance, registered telemarketers should receive preferential rates, provided they follow all guidelines, including proper opt-out mechanisms and DND lists.

5. **Data Monitoring and Reporting:**

- **Monitoring Usage Patterns:** Access Providers should monitor UCC volumes through automated systems, generating reports and alerts when thresholds are crossed, and applying differential tariffs as needed.

Conclusion:

Introducing **differential tariffs for SMS and voice calls beyond a certain limit** is a highly effective tool for disincentivizing UCC through UTM. This approach creates a **direct financial burden** on entities sending mass unsolicited communications, encouraging them to either reduce their UCC volumes or formalize their operations by registering and adhering to regulations. It also helps protect consumers from spam while promoting responsible communication practices. This strategy can be aligned with broader regulatory measures and technological solutions to further reduce the UCC menace.

Q.14 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.

Comments :

Voice Calls :

If a **differential tariff for voice calls** is introduced to disincentivize Unsolicited Commercial Communication (UCC), determining the right limit is critical. This limit should strike a balance between curbing abuse and allowing legitimate business communications to function effectively. Here's how you can set the limit and some considerations for doing so:

Considerations for Setting the Limit:

1. Industry Norms and Average Usage:

- Study the typical call volume for legitimate businesses. Many businesses, such as customer service centers, need to make a significant number of calls. The limit should be set higher than this typical usage to ensure legitimate businesses are not penalized.

2. Nature of the Business:

- Different industries have varying communication needs. The limit could vary depending on the type of entity (e.g., marketing, service, telehealth) or the purpose of the calls (e.g., customer service, promotional campaigns). Entities sending promotional calls may need a stricter limit compared to customer service lines.

3. Current UCC Patterns:

- Analyze the volume of voice calls made by UTM's who frequently engage in UCC. The limit should be set to target high-volume spammers while still allowing moderate business communication.

4. Duration and Frequency:

- Consider not just the number of calls but also the **duration** and **frequency**. Spammers often make very short calls, while legitimate calls may have longer durations. Therefore, both call counts and average duration should be considered.

5. **Consumer Feedback and Complaints:**

- Analyze the **complaint patterns** related to unsolicited calls, such as frequency and volume thresholds that lead to complaints. The limit can be set at a point where consumer inconvenience typically begins.

Potential Limit for Differential Tariffs:

1. **For Promotional Voice Calls:**

- A **daily limit** of 500 to 1000 calls per day per telemarketer could be introduced. Once this limit is crossed, a **higher tariff** could apply to additional calls. This limit allows businesses to make reasonable numbers of calls but dissuades mass spamming.
- For **monthly limits**, around **10,000 to 20,000 calls** per month could be reasonable before applying differential tariffs.

2. **For Other Types of Voice Calls** (e.g., Customer Support):

- Customer support or service-related calls could have a **higher threshold** (e.g., 2000-3000 calls per day) before differential tariffs apply since these businesses might have legitimate needs for higher volumes.

3. **For Short-Duration Calls:**

- If a call is shorter than **30 seconds** (indicating a potential spam call or a hang-up), a differential tariff could be introduced after a smaller limit, such as **100-200 calls per day**, because such calls often represent UCC patterns.

Graduated Tariff Structure:

- Instead of a flat rate increase, a **graduated tariff structure** could be applied:
 - **Up to 1000 calls per day:** Standard tariff.
 - **1000-2000 calls per day:** 1.5x the standard tariff.
 - **2000+ calls per day:** 2x the standard tariff.
 - For calls above **30,000 per month**, a **steeper increase** (e.g., 3x) could be implemented.

Additional Monitoring:

- UTM's reaching the differential tariff limit frequently should be subject to **increased scrutiny** and flagged for potential regulatory action.
- **Exemptions** could be considered for certain essential services (e.g., emergency or healthcare communication).

Conclusion:

A **limit of 500 to 1000 calls per day per telemarketer** for promotional calls is a reasonable threshold for introducing differential tariffs, depending on the business model and the nature of the calls. Beyond this, businesses would need to pay progressively higher rates, disincentivizing mass UCC while allowing legitimate businesses to operate.

SMS :

If a **differential tariff for SMS** is introduced to disincentivize Unsolicited Commercial Communication (UCC), the limit should balance allowing legitimate business communications while curbing mass

spamming by Unregistered Telemarketers (UTMs). Here's how the limit could be structured for SMS:

Considerations for Setting the Limit:

1. Industry Norms for Legitimate SMS Traffic:

- **Transactional SMS:** Legitimate transactional messages (e.g., OTPs, payment confirmations) need to flow freely without facing penalties. These generally have higher volumes but are essential for user experience.
- **Promotional SMS:** Marketing and promotional SMS traffic is typically where UCC issues arise. These have higher volumes and less criticality.

2. Consumer Tolerance:

- SMS spam is often tolerated less than call spam because it's easier to inundate consumers with bulk messages. This means the limit for promotional messages should be stricter.

3. Patterns of UCC via SMS:

- UTMs tend to send **bulk SMS in high volumes**. Studying the message volume patterns and complaint data could help establish a limit that targets UTMs while allowing legitimate communication.

4. Frequency of SMS Campaigns:

- Frequency is an important factor. Businesses that send SMS campaigns frequently should face stricter limits, as repeated SMS blasts are often a source of consumer frustration.

5. Message Content and Purpose:

- Differentiating between **transactional SMS** (e.g., banking alerts, e-commerce updates) and **promotional SMS** (e.g.,

marketing offers) is crucial, as the former is often exempt from such regulations.

Potential Limit for Differential Tariffs for SMS:

1. For Promotional SMS:

- A **daily limit of 500-1000 SMS per day per telemarketer** could be reasonable for promotional messages. Beyond this limit, a **differential tariff** can be applied. This would allow legitimate businesses to send out reasonable volumes of marketing material while deterring mass spamming by UTM.
- On a **monthly basis**, the limit could be set at **10,000 to 20,000 SMS** per telemarketer. Once this threshold is reached, the differential tariff would kick in for any additional messages.

2. For Transactional SMS:

- **Higher limits or exemptions** could be provided for transactional SMS, as these are typically more necessary for business operations (e.g., OTPs, alerts). These messages may not need to be subject to the same limits as promotional SMS, given their nature and importance.

3. For Short-Duration Bulk SMS Campaigns:

- If a business sends a high volume of **identical or near-identical messages** (e.g., marketing campaigns) within a short period (e.g., within an hour), a lower limit could apply. A threshold of **200-300 SMS per hour** may be set for such bulk messages, beyond which a differential tariff could be introduced.

Graduated Tariff Structure:

- The differential tariff could be applied in a **graduated manner**:

- **Up to 1000 SMS per day:** Standard tariff.
- **1000-2000 SMS per day:** 1.5x the standard tariff.
- **2000+ SMS per day:** 2x the standard tariff.
- For **30,000+ SMS per month**, the tariff could escalate further (e.g., 3x the standard rate).

Additional Monitoring:

- **UTMs crossing the limit** frequently or sending a large volume of messages within a short period should be flagged for review and potential regulatory action.
- **Incentives for registration:** Registered telemarketers could receive more lenient limits or lower tariffs if they follow compliance guidelines, while unregistered telemarketers (UTMs) would face stricter limits and higher tariffs.
- **Exemptions for essential services:** Organizations involved in **critical or emergency services** (e.g., healthcare alerts, government notifications) should be exempt from these limits to ensure uninterrupted service.

Conclusion:

A **limit of 500 to 1000 SMS per day** for promotional messages is a reasonable threshold for introducing differential tariffs, with **higher tariffs** applied for larger volumes. This approach discourages mass UCC through UTMs while still allowing legitimate businesses to operate. Transactional SMS and essential services should be treated differently, with higher limits or exemptions.

Q.15 If differential tariff is introduced, what could be the tariff beyond a limit for:

i. Voice calls.

ii. SMS.

Please justify with rationale.

Comments :

Voice Calls :

If a **differential tariff** is introduced for voice calls to curb Unsolicited Commercial Communication (UCC), the specific tariff structure beyond a set limit should be designed to **disincentivize mass calling** while still allowing legitimate businesses to operate. Here's how the tariff structure could be implemented:

1. Tariff Structure Beyond a Set Limit:

A **graduated tariff** can be applied, increasing progressively as the number of voice calls exceeds the predefined limit. This would ensure that bulk callers (especially UTMs) face higher costs while moderate or legitimate business operations are less affected.

Example Structure:

- **Up to 1000 calls per day:** Standard tariff (e.g., ₹0.10 per call or current prevailing rate).
- **1001 to 2000 calls per day:** 1.5x the standard tariff (e.g., ₹0.15 per call).
- **2001 to 5000 calls per day:** 2x the standard tariff (e.g., ₹0.20 per call).

- **5001 to 10,000 calls per day:** 3x the standard tariff (e.g., ₹0.30 per call).
- **10,000+ calls per day:** 4x or higher (e.g., ₹0.40 per call).

This structure would apply on a **daily basis**, and a similar structure could be applied on a **monthly basis** as well:

- **Up to 20,000 calls per month:** Standard tariff.
- **20,001 to 50,000 calls per month:** 2x the standard tariff.
- **50,001+ calls per month:** 3x or more.

2. Penalty for Excessive Short-Duration Calls:

Spammers and UTMs often make **short-duration calls** (e.g., hang-ups or missed calls). To prevent abuse of short-duration calls, a higher tariff could be applied for calls lasting **less than 30 seconds**:

- **Short-duration calls** (less than 30 seconds): 1.5x or 2x the standard tariff after 500 short calls per day.

This helps dissuade entities from exploiting the low cost of short calls to mass dial consumers.

3. Higher Tariff for Specific Call Types:

- **Promotional or marketing voice calls** should have a **stricter differential tariff** structure than other types of calls (e.g., customer service, informational calls). For example:
 - Promotional calls above 1000 calls per day could incur a **2x tariff immediately**, while transactional or informational calls could see a lower multiplier.

4. Incentives for Registered Telemarketers (RTMs):

- Registered Telemarketers (RTMs) could enjoy **lower multipliers** if they comply with regulations, such as adhering to **Do Not Disturb (DND)** lists, using approved messaging templates, and other best practices. For example:
 - **Registered RTMs:** 1.5x tariff above the threshold.
 - **Unregistered Telemarketers (UTMs):** 2x or higher immediately after crossing the limit.

5. Surcharge for Violating Regulations:

- In addition to differential tariffs, **penalties or surcharges** could be introduced for entities violating **Telecom Commercial Communications Customer Preference Regulations (TCCCPR)**:
 - ₹1 per call surcharge for each call that violates **DND regulations**.
 - Additional **fin**es for non-compliant entities beyond a certain number of violations, leading to **suspension or blacklisting** after repeated breaches.

6. Cap on Discounts:

- UTMs or bulk callers may try to exploit bulk discounts offered by telecom service providers. There could be a **cap on discounts** for bulk callers that send or make calls beyond a certain limit. For instance, beyond **50,000 calls per month**, discounts should be minimized or eliminated to ensure that UTMs do not misuse pricing schemes.

Conclusion:

A differential tariff system for voice calls beyond a certain limit could follow a **graduated approach**, starting with a small increase (1.5x) after 1000 calls per day and escalating to 2x or more for larger volumes (5000+ calls). The use of **short-duration calls** should attract higher tariffs, and **registered telemarketers** could benefit from more favorable tariffs compared to **unregistered entities**. This structure would dissuade excessive UCC while ensuring legitimate businesses can continue their operations affordably.

SMS :

If a **differential tariff for SMS** is introduced to curb **Unsolicited Commercial Communication (UCC)**, the tariff should increase progressively as the number of messages exceeds a set limit. The objective is to disincentivize bulk SMS spamming by **Unregistered Telemarketers (UTMs)** while allowing legitimate businesses to function.

1. Graduated Tariff Structure Beyond a Set Limit:

A **graduated tariff** can be applied for SMS beyond a daily or monthly threshold. Below is a potential structure:

Example Tariff Structure (per SMS):

- **Up to 1000 SMS per day:** Standard tariff (e.g., ₹0.05 per SMS or current prevailing rate).
- **1001 to 5000 SMS per day:** 1.5x the standard tariff (e.g., ₹0.075 per SMS).
- **5001 to 10,000 SMS per day:** 2x the standard tariff (e.g., ₹0.10 per SMS).

- **10,001 to 20,000 SMS per day:** 3x the standard tariff (e.g., ₹0.15 per SMS).
- **20,000+ SMS per day:** 4x or higher (e.g., ₹0.20 per SMS).

For monthly limits, similar structure:

- **Up to 30,000 SMS per month:** Standard tariff.
- **30,001 to 50,000 SMS per month:** 1.5x the standard tariff.
- **50,001 to 100,000 SMS per month:** 2x the standard tariff.
- **100,000+ SMS per month:** 3x or higher.

This structure would ensure that the cost of sending large volumes of SMS increases significantly as the volume grows, deterring UTMs from spamming.

2. Penalties for High-Frequency Bulk SMS Campaigns:

For businesses or entities sending **bulk SMS campaigns** (e.g., identical promotional messages) within a short time frame (e.g., within an hour or day):

- **Threshold:** For instance, if more than 500 identical SMS are sent in one hour, apply a **surcharge of 2x the standard rate** for the next 500 SMS.
- **Higher tariffs** should kick in for short-duration, high-volume bulk SMS campaigns, which are common in UCC.

3. Increased Tariff for Promotional SMS:

Promotional SMS, especially from UTMs, should be subject to **stricter tariff increases:**

- For **promotional SMS**, the **tariff increase** could begin after **500 SMS per day**. For instance:
 - **Up to 500 SMS per day**: Standard tariff.
 - **501 to 1000 SMS per day**: 2x the standard tariff.
 - **1001 to 5000 SMS per day**: 3x the standard tariff.
 - **5001+ SMS per day**: 4x the standard tariff.

This ensures that promotional spam is discouraged more aggressively than transactional or informational SMS.

4. Surcharge for Non-Compliant SMS (e.g., violating DND):

- For each SMS that violates **Do Not Disturb (DND)** regulations or customer preferences, a **surcharge** could be added to the base tariff (e.g., ₹1 per non-compliant SMS).
- **Repeat violations** could result in even higher tariffs or penalties.

5. Lower Tariffs for Registered Telemarketers (RTMs):

- **Registered Telemarketers (RTMs)** who comply with **Telecom Commercial Communications Customer Preference Regulations (TCCCPR)** could receive more favorable tariffs compared to UTM. For instance, RTMs might face a **lower multiplier** (e.g., 1.5x after 1000 SMS) compared to UTM, who could face **2x or higher tariffs immediately after exceeding 500 SMS**.

6. Cap on Bulk Discounts:

UTMs may try to exploit bulk SMS discounts. To prevent this:

- **Bulk discount caps** should be introduced for businesses exceeding a certain threshold (e.g., 20,000 SMS per day). Beyond this limit,

discounts should be reduced or eliminated to dissuade excessive spamming.

Conclusion:

A **differential tariff for SMS** beyond a reasonable limit should follow a **graduated structure**, with rates increasing progressively as the SMS volume exceeds daily or monthly thresholds. For example, starting with a **1.5x tariff beyond 1000 SMS per day**, increasing to **3x or 4x** for higher volumes (e.g., 10,000 SMS per day). This structure would **disincentivize bulk SMS spamming**, especially by UTM, while allowing legitimate businesses to communicate within reasonable limits.

Q.16 Whether differential tariff should be introduced in a graded manner? If so, please suggest the methodology with justification.

Comments :

Introducing differential tariffs in a graded manner for unsolicited commercial calls (UCC) could be a strategic approach, but it requires careful consideration. Here are key factors to weigh:

1. Incentivizing Compliance

Differential tariffs could be used to encourage compliance among businesses and telemarketers. For instance, higher tariffs could be imposed on repeat offenders or businesses that frequently violate rules on unsolicited commercial communication. This would act as a deterrent and motivate companies to respect consumer preferences and avoid harassment.

2. Tiered Penalties Based on Violation Severity

The graded tariff structure could be based on the severity of the violation.

For example:

- **Minor violations** (accidental breaches or first-time offenders) could face lower penalties.
- **Severe violations** (repeated offenses or intentional breaches) could attract significantly higher tariffs, reflecting the seriousness of the violation.

3. Encouraging Smaller Businesses

A graded tariff could benefit smaller businesses or start-ups, making it affordable for them to conduct necessary promotional activities while adhering to regulatory norms. Larger corporations with higher volumes of calls and potential to cause more disturbances could be charged higher tariffs for violations, reflecting their greater impact.

4. Mitigating Consumer Harassment

A graded approach could also be tailored based on the impact on consumers. For example:

- **Calls made during inappropriate hours** or those repeatedly disturbing the same consumer could attract higher tariffs.
- **Mass commercial calling campaigns** that affect a large number of people could be subject to higher tariffs compared to smaller, more targeted campaigns.

5. Administrative Feasibility

Implementing a differential tariff system for UCC would require robust monitoring and enforcement mechanisms. It may also raise concerns about

how to objectively determine the tariff level for each violation. Clear guidelines would need to be established to avoid confusion and ensure transparency.

Conclusion

A graded tariff system for UCC could incentivize compliance, mitigate consumer harassment, and address the needs of both large and small businesses. However, it must be carefully structured to avoid excessive complexity, ensuring that penalties are proportional to the nature and frequency of the violation.

Careful Consideration :

Introducing differential tariffs in a graded manner for unsolicited commercial calls (UCC) requires careful consideration across several dimensions to ensure the system is fair, effective, and sustainable. Here are key aspects that should be carefully considered:

1. Regulatory Framework and Compliance

- **Clarity in Rules:** The criteria for graded tariffs must be clearly defined. For example, what constitutes a minor versus a major violation? These definitions should be explicit to avoid ambiguity and ensure businesses understand the penalties.
- **Regulatory Compliance:** Existing guidelines, such as the Telecom Commercial Communications Customer Preference Regulations (TCCCPR), must be taken into account to ensure the differential tariff system aligns with current frameworks.

- **Legal Safeguards:** Ensure that the differential tariff system complies with data protection and consumer rights laws. The framework should be legally defensible to avoid challenges in courts.

2. Consumer Impact and Protection

- **Consumer Harassment Levels:** Tariffs should reflect the level of inconvenience or harassment caused to consumers. Calls made at inappropriate hours or repeated calls should attract higher penalties to discourage these practices.
- **Consumer Preferences:** The system should protect consumers who have opted out of promotional calls through mechanisms like Do Not Disturb (DND) services. Violations of these preferences should incur heavier penalties.

3. Business and Economic Impact

- **Scalability for Different Business Sizes:** Tariff structures should be proportional to the size of the business. Small and medium enterprises (SMEs) may find it difficult to pay high penalties, so a more lenient tariff structure for minor infractions by small businesses could be considered.
- **Impact on Telemarketing:** While discouraging non-compliance is important, tariffs should not discourage legitimate business activities. The framework should strike a balance between penalizing unsolicited calls and allowing businesses to reach out to potential customers within legal limits.

4. Gradation Based on Violation Severity

- **First-Time vs. Repeat Offenders:** The tariff system should differentiate between first-time offenders and repeat violators. First-time offenders may face lower fines, while repeat violators or those committing more serious infractions should be subject to higher tariffs.
- **Nature of Calls:** Differentiate based on the scale and frequency of the calls. Mass calling campaigns that disrupt thousands of consumers should incur higher tariffs than smaller, targeted campaigns.

5. Implementation and Monitoring

- **Enforcement Mechanisms:** The regulatory body (such as TRAI in India) must have the tools to effectively monitor and enforce the tariff system. This could include tracking call records, auditing telemarketers, and having a complaint resolution system in place.
- **Automated Monitoring Systems:** Leveraging technology like AI and machine learning to detect patterns in call data can help identify violators and apply the appropriate tariffs without overburdening human resources.

6. Transparency and Accountability

- **Transparency in Application:** The tariff structure should be transparent, and businesses should know exactly how tariffs are calculated based on the nature and frequency of violations.
- **Accountability for Telemarketers:** Ensure that telemarketing companies are accountable for keeping accurate records of calls made and consumer preferences.

7. Consumer Awareness and Feedback Mechanisms

- **Consumer Education:** Consumers should be educated about their rights concerning UCC, such as opting out of calls, and how to report violations.
- **Feedback Systems:** Implement feedback and grievance mechanisms for consumers to easily report violations and provide data for tariff enforcement.

8. Technological Infrastructure

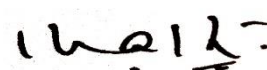
- **Call Monitoring Tools:** Develop robust technological systems that can track unsolicited commercial calls and monitor compliance with the regulations.
- **Data Privacy:** Ensure that while tracking and monitoring, the privacy of consumers is protected, in line with relevant data protection laws.

Conclusion

Careful consideration of the regulatory framework, business impact, consumer protection, enforcement mechanisms, and technological infrastructure is crucial when introducing a differential tariff system for UCC. The goal is to discourage unwanted calls without unduly burdening legitimate business activities, while also safeguarding consumer rights and preferences.

Thanks.

Sincerely Yours,



(Prof. Dr. Kashyapnath)
President