CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT

Comments on

Consultation on Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026.

Spam and Unsolicited Commercial Communications as Vectors for Fraud, Impersonation, and Cybercrime

Executive summary:

Spam and Unsolicited Commercial Communications (UCC)—especially phone calls and SMS—are not merely "nuisance." In modern cybercrime, they function as a **high-reach, low-cost initial access channel** that attackers use to (a) impersonate trusted institutions, (b) harvest credentials and OTPs, (c) hijack phone numbers (SIM swap/port-out), and (d) trigger downstream financial fraud and account takeover. This pattern is reflected in India's scale of telecom spam reporting and cybercrime response systems, and in global consumer protection statistics that show large losses to imposter scams and text-initiated scams.

India's official ecosystem already contains several building blocks relevant to combating UCC-enabled fraud: (i) complaint channels (e.g., 1909), (ii) a DLT-based compliance architecture under TCCCPR, (iii) TRAI technology-forward enforcement (e.g., AI/ML detection directions for suspected UCC), and (iv) government cybercrime response mechanisms (1930 / CFCFRMS) and infrastructure actions (e.g., blocking incoming international spoofed calls).

The central policy challenge is to **tighten trust and traceability** in telecom-origin communications—without harming legitimate businesses, critical service messaging, or digital inclusion. This requires a layered design: (1) enforceable consent and identity controls, (2) telecom-grade call/SMS authentication and filtering, (3) strong SIM/port security and OTP alternatives, and (4) due process and false-positive safeguards (appeals, audit trails, transparency). International approaches provide workable patterns: US STIR/SHAKEN call authentication and robocall enforcement; UK blocking of international calls spoofing domestic numbering and strengthened CLI guidance; consent-based direct marketing frameworks in Singapore, Australia, Canada, and the EU.

How UCC enables fraud and cybercrime:

Telecom spam becomes a fraud vector because it combines (i) **real-time human manipulation**, (ii) **UI trust cues** (familiar numbers, known brands), and (iii) **control-plane weaknesses and provisioning processes** (SIM replacement/porting), enabling attackers to "bridge" from unsolicited outreach to verified financial actions.

Major attack types, with evidence-based examples:

Caller impersonation and "authority" fraud (vishing + spoofing). Attackers pose as banks, regulators, government agencies, or service providers, using urgency ("account blocked," "KYC update," "refund pending," "investigation") to extract OTPs, passwords, or payments. Government advisories and public awareness materials repeatedly emphasize that legitimate institutions do not solicit sensitive information via unsolicited calls/messages.

Smishing (SMS phishing) to capture credentials/OTPs or deploy malware. Smishing uses SMS links and "click-to-fix" narratives. India's National Cyber Crime Reporting Portal hosts advisories covering smishing and related patterns, and UK guidance treats texts as a common phishing channel requiring strict business messaging hygiene.

SIM swap / SIM re-issue hijack (account takeover via mobile number control).
In SIM swap, an attacker convinces or corrupts the SIM issuance / replacement workflow so the victim's number is moved to an attacker-controlled SIM/eSIM—allowing interception of OTPs and account recovery messages and enabling rapid funds transfer. India's CERT-In has issued guidance on SIM swap fraud risks and mitigations.

OTP interception and redirection (beyond SIM swap). Even without SIM swap, attackers can redirect OTPs by (a) call forwarding/social engineering, (b) device compromise, or (c) network-level interception in legacy signaling environments. Authoritative technical sources

(NIST, ITU) explicitly caution that PSTN-based OTP delivery can be intercepted or redirected and recommend alternative authenticators and risk checks (e.g., detecting SIM change/porting).

Business compromise chains involving mobile vectors (smishing→account takeover→payment fraud/BEC). While classic Business Email Compromise (BEC) is "email-native," credential theft and account takeover can originate from phishing broadly (including texts and calls) and then pivot into invoice fraud, payroll redirection, and vendor payment diversion. Global law enforcement highlights BEC as a major loss driver.

AI-voice and deepfake-assisted vishing (impersonation at scale). Recent law-enforcement alerts document the use of AI-generated voice messages and combined smishing/vishing to impersonate officials and move victims to secondary channels. Regulators also recognize AI-generated voices as falling under robocall restrictions.

Why UCC is structurally attractive to attackers?

UCC's fraud value is amplified by a few recurring dynamics:

- **Trust transference:** Users tend to trust phone numbers and familiar brand identifiers more than web/email signals, especially when caller ID is spoofed to look local or authoritative.
- **Time pressure:** Calls enable live coercion and "on-the-spot" manipulation, increasing OTP sharing and remote access installation.

- **Account recovery dependence:** Many services still rely on SMS/voice OTP for login recovery; NIST flags this channel as riskier and recommends considering SIM/port change indicators before using PSTN-based out-of-band secrets.
- **Cross-border spoofing:** International call origination and VoIP interconnection allow "cheap spoofing," which is why regulators increasingly require blocking international calls that present domestic numbering, and why India has moved to block incoming international spoofed calls.

Attacker mechanics in telecom and digital ecosystems:

This section maps the technical mechanisms that enable the above attacks, focusing on implementable control points.

Caller-ID spoofing and CLI manipulation:

At the core of many vishing scams is **Calling Line Identification (CLI) spoofing**, commonly executed through VoIP systems and interconnect pathways. US regulators promote call authentication frameworks (STIR/SHAKEN) designed to validate call origin information across networks and support downstream blocking/labeling decisions.

The UK model is particularly operational: telecom providers are expected to block international calls that present UK numbers (except narrow legitimate cases), backed by updated CLI guidance and enforcement programs.

India has similarly recognized this risk in the context of international spoofed calls, with DoT/TSP systems to identify and block incoming international spoofed calls.

Signaling-layer risks (SS7 / interconnect security) enabling SMS interception and subscriber fraud:

Legacy mobile signaling and interconnect environments (SS7 and SS7-like interfaces) can be abused for **SMS interception, spoofing, and subscriber fraud**, especially where networks lack robust interconnect monitoring and firewalling. ITU's technical work on SS7 vulnerabilities explicitly discusses these attack classes and mitigation measures for digital financial services.

Operator-side mitigation patterns include SS7 traffic monitoring, anomaly detection, and firewalls described in industry security guidance, and surveyed at EU level.

SIM re-issuance, SIM swap, and number porting abuse:

Fraudsters exploit operational workflows (customer support, retail KYC gaps, forged documents, insider compromise) to execute SIM swap or unauthorized reissue. ITU recommendations explicitly connect SIM swaps and number porting to increased fraud risks in ecosystems that rely on SMS OTP/USSD.

India's CERT-In advisory underscores the consumer/account takeover risk of SIM swap fraud and recommends protective actions.

Device-level compromise and SMS-forwarding/credential theft:

Smishing links can lead to credential capture, malicious app installs, or abuse of accessibility permissions—allowing OTP capture, call/SMS forwarding, or remote control. Public safety guidance (including official and quasi-official handbooks) identifies smishing/vishing as standard modes of phishing and warns of mobile-based malware and credential theft.

Number recycling as an account takeover vector:

When telecom numbers are disconnected and later reassigned, legacy account recovery implementations can unintentionally send OTPs and sensitive account resets to new users of recycled numbers. This risk is documented in peer-reviewed empirical work and is the reason standards bodies caution against over-reliance on SMS for authentication and recovery.

Consumer harm and metrics:

India-relevant indicators:

Spam/UCC volume and channel distribution. Government releases describe millions of spam call/SMS reports and substantial UCC complaint volumes, illustrating the scale of unwanted telecom-origin communications.

Cybercrime scale and response outcomes. Government reporting reflects sharp growth in reported cybersecurity incidents and large-scale disruption actions (e.g., blocking SIM cards/IMEIs linked to fraud), indicating both expanding threat volume and increasingly active interventions.

Financial fraud reporting and "rapid response" savings. India's Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) and the 1930 helpline are repeatedly described as enabling rapid intervention to stop fund siphoning, with reported cumulative savings and large complaint volumes.

Payment fraud as predominantly social engineering/phishing-driven (policy-relevant).

Parliamentary committee evidence indicates that many payment frauds are understood to be phishing in various forms (including vishing and smishing) and also highlights concerns about over-reliance on OTP-based models.

Global consumer harm metrics that inform regulatory proportionality:

Global consumer protection and law-enforcement datasets consistently show large reported losses tied to impersonation and text/call-driven scams:

- US consumer protection data reports **hundreds of thousands of imposter scam reports** with multi-billion-dollar losses, indicating impersonation is a major consumer harm class.
- US data specifically on "text-initiated" scams reports **hundreds of millions of dollars in annual losses**, underscoring the rising economic impact of SMS-origin scams.
- US law enforcement's IC3 annual reporting reflects **very large aggregate losses** and highlights BEC and other forms of cyber-enabled financial fraud as major drivers.

Interpretation (policy-relevant): voice calls dominate reported spam volumes, meaning anti-fraud controls must treat **voice** as a first-class risk surface (authentication, spoof detection, and consumer-facing trust signals), not only SMS filtering.

Preventive measures and policy design:

A compliance-ready anti-UCC-and-fraud posture should be designed as **layered controls** with clear accountability, auditability, proportionality, and inclusion. The measures below are framed as implementable obligations that can be distributed across access providers (TSPs/ASPs), telemarketers, principal entities, and digital ecosystem stakeholders (banks, wallet providers, platforms).

Prevention measures comparison table:

Measure	Targeted threat(s)	Implementation complexity	Consumer impact	Legal/regulatory requirement	Priority
Network-level caller-ID authentication (STIR/SHAKEN-like for IP interconnect)	CLI spoofing, impersonation vishing	High	High positive (trust, fewer spoofed calls)	DoT/TRAI mandate + interoperable standards	P0
Inbound international spoofing blocks (domestic CLI presented from abroad)	Cross-border spoofing, IRS/bank impersonation-style fraud	Medium	High positive; risk of false positives if poorly scoped	DoT direction + measurable exemptions	P0
Robust CLI	Spoofing via	Medium	High positive;	License	P0

Measure	Targeted threat(s)	Implementation complexity	Consumer impact	Legal/regulatory requirement	Priority
integrity rules and gateway provider due diligence	gateway routing		protects vulnerable groups	conditions + enforcement audits	
SMS sender/headers + template controls with rapid takedown	Smishing, brand impersonation, malicious links	Medium	High positive; fewer fake “KYC/update” scams	TCCCPR/DLT strengthening	P0
SIM swap / SIM re-issue hardening (step-up verification + cooling-off)	SIM swap, OTP interception	Medium–High	High positive; short-term friction	DoT KYC rules + TRAI coordination	P0
Port-out lock and high-risk change alerts (SIM/port change notifications)	Porting abuse, account takeover	Medium	High positive	Telecom Act user-protection powers + operator SOPs	P0
SS7/Diameter interconnect monitoring + firewalls	SMS interception, location/SMS fraud	High	High positive but invisible	Security obligations + audit	P1
“Risk signal API” for verifiers (SIM change/porting/tenure checks)	OTP fraud, account recovery abuse	Medium	High positive; reduces fraud without new UX	Regulatory enabling + privacy safeguards	P1
Alternatives to SMS OTP for high-risk use cases (FIDO/passkeys, app push, TOTP)	OTP interception, number recycling	Medium	High positive; inclusion concerns if not designed well	RBI/sector rules + standards guidance	P1

Measure	Targeted threat(s)	Implementation complexity	Consumer impact	Legal/regulatory requirement	Priority
Number recycling safeguards (minimum quarantine, rebind controls)	Account takeover via recycled numbers	Medium	High positive; reduces accidental account access	Operator policy + ecosystem coordination	P2
Standardized "verified business messaging" and safe content principles	Smishing credibility, brand mimicry	Low–Medium	Positive; improves trust	Codes of practice + enforcement	P2
Consumer-facing consent dashboards + easy opt-out	Unwanted marketing; reduces attack surface by shrinking target list	Medium	High positive for privacy/choice	DPDP-consistent consent design + TCCCPR alignment	P1
"Rapid fraud takedown" playbook linked to national cybercrime helpline	Ongoing scam campaigns	Medium	High positive; speed reduces losses	Inter-agency SOPs; due process	P0
Transparent appeals + false-positive review	Overblocking risks	Medium	Prevents legitimate communications disruption	Procedural safeguards in regulations	P0
Strong penalties + joint liability for repeat violators	Industrial-scale spam/fraud ecosystems	Medium	High deterrence; fairness needed	Updated penalty schedule + adjudication	P0

The “why this is implementable” and evidence grounding for the key control types are established in the public regulatory/standards record: call authentication and robocall mitigation is a core FCC approach; UK operationalizes spoofing control via CLI guidance and provider obligations; NIST and ITU warn about SMS OTP risk and enumerate SIM swap/SS7 mitigations; India has already deployed inbound spoof blocking and UCC complaint/detection frameworks.

Detection-to-enforcement workflow flowchart:

This flow depicts an end-to-end workflow that aligns with DLT-based traceability/logging and adds “fraud-first” escalation pathways with due process and audit trails. (The architecture is consistent with the existence of complaint channels and enforcement mechanisms, and with technology-enabled detection actions already described in Indian telecom and government releases.)

```
flowchart TD
 A[Consumer receives call/SMS] --> B{User trusts message?}
 B -->|No| C[Ignore/block locally]
 B -->|Unsure / suspicious| D[Report via 1909 / DND app / web portal]
 D --> E[TSP/ASP logs complaint + metadata]
 E --> F[DLT linkage: header/template/PE/TM mapping]
 E --> G[Network analytics + AI/ML detection triggers]
 F --> H{Classification}
 G --> H
 H -->|UCC violation| I[Automated containment: suspend sender/header,
```

```
stop templates]
 H -->|Suspected fraud| J[High-severity containment: block resources + flag patterns]
 J --> K[Share indicators with CFCFRMS/1930 + LEA nodal channel]
 I --> L[Notify Principal Entity + Telemarketer; require corrective action]
 J --> L
 L --> M[Adjudication with audit trail]
 M --> N{Appeal filed?}
 N -->|Yes| O[Time-bound appeal review + false-positive checks]
 N -->|No| P[Finalize penalties/blacklisting]
 O --> P
 P --> Q[Publish transparency metrics + feedback to detection models]
```

Risk/benefit design principles (proportionality, due process, inclusion)

Proportionality:

Controls should be strongest where harm is highest (financial services impersonation, OTP capture, SIM swap), while low-risk marketing compliance is handled through predictable consent/opt-out processes and automated compliance tooling. This aligns with the observed heavy losses in impersonation and text/call-driven fraud categories and with the recognized vulnerability of PSTN-based OTP channels.

Due process + false-positive safeguards:

Because network-level blocking can disrupt legitimate enterprises and critical messages, regulatory design should require: (i) measurable blocking criteria, (ii) time-bound review, (iii) audit trails for each action (which entity, which

template/header, what evidence), and (iv) an accessible appeals process. UK practice explicitly identifies enforcement programs and operational guidance, and India's own technology-led enforcement directioning implies the need for measurable accuracy and accountability.

Inclusion (MSMEs and non-smartphone users): For MSMEs, compliance costs can be a barrier—so tooling must be accessible (lightweight registration, standardized templates, bulk onboarding support), and enforcement should distinguish between negligent noncompliance and organized abuse. For non-smartphone users, do not assume app-only controls: maintain voice/SMS complaint options (e.g., 1909) and consider verified voice cues (e.g., "verified caller" indicators) rather than relying solely on app-based authentication.

Phased implementation roadmap:

Short term (0–6 months): "Stop the bleeding" controls

- ✓ Expand and standardize inbound spoof blocking with transparent exception handling and measurement to minimize false positives.
- ✓ Mandate rapid takedown of reported fraudulent headers/templates and integrate UCC enforcement with cybercrime escalation channels (1930/CFCFRMS) for suspected fraud campaigns.
- ✓ Implement SIM swap/port-out "high-risk event" controls: step-up checks, delays for high-risk changes, and proactive alerts.
- ✓ Publish transparency metrics: complaint volumes, actions taken, appeal outcomes, false-positive rates, and response SLAs.

Medium term (6–18 months): "Trust infrastructure"

- Roll out call authentication for IP interconnects and enterprise-origin calls; create a consistent verified-caller UX.
- Deploy SS7/Diameter monitoring and firewalling as audited minimum baselines.
- Reduce dependence on SMS OTP for high-value transactions; align authentication guidance with recognized standards (risk checks for SIM/port events and movement to stronger authenticators).

Long term (18–36 months): "Resilient ecosystem"

- Institutionalize cross-regulator coordination (telecom–banking–law enforcement) and data-sharing protocols with privacy safeguards.
- Formalize number recycling protections and account re-binding security norms based on empirical findings.
- Integrate AI-voice risk into both robocall/telemarketing compliance and anti-fraud controls, consistent with regulator recognition that AI-generated voices fall under existing restrictions.

International comparisons and draft regulatory prescriptions:

Comparative international practices and lessons for India:

United States (FCC + consumer protection datasets). The US approach combines:

(i) network-level call authentication (STIR/SHAKEN) and robocall mitigation, and

(ii) (ii) consumer protection enforcement recognizing the evolution of AI-generated voice in robocalls under existing legal restrictions. The evidence base includes FTC and IC3 reporting that quantifies losses across scam types, supporting proportionate yet firm intervention.

United Kingdom (Ofcom + ICO). The UK operationally targets spoofing by requiring providers to block international calls that falsely present UK numbering, with published guidance and enforcement programs. Separately, the ICO enforces marketing rules with monetary penalties for nuisance/spam messages, emphasizing consent records and lawful marketing operations. This two-regulator model (telecom + privacy/marketing enforcement) offers a useful division of labor for India between telecom regulation and broader consumer/data protection enforcement.

Singapore (PDPC DNC registry). Singapore's DNC regime centers on "clear and unambiguous consent" exceptions, and its guidelines emphasize that telemarketing consent collection itself is regulated (i.e., you cannot bypass the DNC rules by seeking consent via prohibited telemarketing methods). This is a strong anti-dark-pattern model relevant to preventing "consent laundering" and coerced opt-ins.

Australia (ACMA Spam Act enforcement). Australia's compliance rules are simple, compliance-ready, and

enforcement-oriented: obtain consent, identify the sender, provide easy unsubscribe, and do not make unsubscribe burdensome (e.g., requiring logins or extra personal data). This is a strong template for minimizing opt-out friction and reducing the pool of reachable victims.

Canada (CRTC CASL). CASL's tripartite requirements—consent, identification, unsubscribe—are a clear compliance baseline, with explicit guidance for businesses. It also covers additional digital threats beyond "marketing annoyance," which is conceptually aligned with treating spam as a cyber risk surface.

European Union (ePrivacy Directive framework). The EU's ePrivacy Directive is the core legal backbone for privacy in electronic communications and restrictions on unsolicited communications. While implementation differs by member state, the directive-level approach anchors the principle that electronic communications privacy and unsolicited marketing controls are fundamental rights-based obligations.

Legal grounding for Indian regulatory drafting:

A defensible Indian approach should explicitly anchor anti-UCC and anti-fraud controls in existing legal duties and consumer rights constructs:

- **Telecommunications Act, 2023:** expressly empowers user protection measures and supports requirements around prior consent/controls in telecom service contexts.

- **TCCCPR, 2018:** establishes the consent/preference framework, complaint channels (e.g., 1909), and DLT-based commercial communications governance.
- **DPDP Act, 2023:** provides legal principles for consent (including withdrawal) and requires privacy-by-design thinking for consent dashboards and preference management systems that reduce unwanted communications and associated fraud exposure.
- **IT Act, 2000:** includes explicit offenses for identity theft and cheating by personation using a communication device/computer resource—directly mapping to spoofing/vishing/smishing impersonation behavior.
- **IT (Intermediary Guidelines) Rules, 2021:** impose due diligence and online safety/accountability obligations on intermediaries, which supports cross-platform cooperation when UCC campaigns move victims to messaging apps or web infrastructure.

Model regulatory text snippets suitable for insertion into TCCCPR-style amendments:

These are "regulatory-style" snippets intended to be implementable and auditable (and to withstand proportionality and due process scrutiny). They are written generically so they can be mapped into the structure of a Third Amendment.

Definition: "Suspected Fraud Communication."

> "Suspected Fraud Communication" means any commercial communication or other telecom-origin communication that, based

on objective indicators recorded by the Access Provider/Platform, is reasonably likely to solicit money, credentials, OTPs, KYC documents, remote access, or other authentication factors by impersonation, deception, or misrepresentation, including through caller ID spoofing, misleading templates/headers, or deceptive URLs.

Obligation: high-severity containment with audit trail and appeal.

Where an Access Provider determines a Suspected Fraud Communication, it shall (a) take proportionate interim measures to prevent continuation (including blocking/suspension of the relevant telecom resources/templates/headers), (b) record the objective indicators and decision rationale in an auditable log, (c) notify the affected Principal Entity/Telemarketer, and (d) provide a time-bound appeals mechanism with documented review and false-positive safeguards.

Obligation: SIM swap / port-out risk controls.

Access Providers shall implement step-up verification, “high-risk event” monitoring, and customer notifications for SIM replacement, eSIM activation, and number porting; and shall provide for time-bound risk holds or cooling-off mechanisms for high-risk changes, subject to exceptions for lawful emergencies and documented customer authentication.

Obligation: inbound spoof blocking baseline.

Access Providers shall block incoming international calls that present domestic numbering identifiers unless the call falls within published exception categories and the originating chain provides verifiable legitimacy signals; all exceptions must be logged and auditable.

Obligation: consent-proof and "easy withdrawal" standard (privacy and choice).

Consent records relied upon for commercial communications must be demonstrable, granular, and revocable through low-friction mechanisms at least as easy as the act of giving consent; consent shall not be bundled or coerced as a condition of service beyond what is strictly necessary.

These provisions are consistent with India's move toward technology-enabled UCC detection and enforcement, and they align with global regulatory patterns that combine (i) authentication and blocking for spoofing, (ii) consent and unsubscribe simplicity, and (iii) strong enforcement with transparency and appeal protections.

Actionable checklist for regulators and operators:

For regulators (TRAI/DoT + coordination bodies)

- ✓ Define "suspected fraud communication" triggers and minimum containment actions with audit and appeal.
- ✓ Mandate and measure spoof-blocking effectiveness (including false positives) for inbound international calls.

- ✓ Require standardized transparency reporting (complaints → actions → outcomes → appeals).
- ✓ Enable privacy-safe "risk signal" sharing (SIM/port change indicators) for high-risk verifiers (banks, wallets) with clear legal basis and minimization.

For operators (TSPs/ASPs)

- ✓ Deploy robust gateway controls (CLI validation, anomaly detection, and documented exceptions) and align with spoof-blocking directives.
- ✓ Harden SIM swap/port workflows (step-up checks, cooling-off for high-risk events, immediate customer alerts).
- ✓ Improve complaint UX and closure speed while preserving evidence and audit trails (1909, apps, web).
- ✓ Implement SS7/interconnect monitoring and firewalls; document baseline controls and submit to audits.

For principal entities and large senders:

- ➢ Adopt "trustworthy messaging" principles: no clickable links for sensitive actions; consistent short codes; clear user education; and secure customer support paths.
- ➢ Move away from SMS OTP for high-risk transactions where feasible; adopt phishing-resistant authentication and recovery controls consistent with standards guidance.

Comments :

Context and consumer-centric regulatory objectives:

As a consumer-facing stakeholder, the guiding policy objectives adopted for the below comments are:

Privacy and consent integrity, ensuring "choice architecture" that is accessible, informed, revocable, auditable, and not easily gamed.

Transparency and explainability, especially where AI/ML triggers enforcement (minimizing false positives while improving deterrence).

Deterrence with due process, ensuring the framework is not only strict against spammers but also procedurally fair (timely notices, reasoned decisions, appeal pathways, proportionate sanctions).

Inclusion and proportionality, so that essential services and MSME/SME senders are protected from undue disruption, while still being held to robust compliance standards.

Forward-looking interoperability, aligning telecom consumer protection with wider digital governance (data protection, intermediary due diligence) and global best practices for consent-based marketing controls.

Evidence base on consumer harm and enforcement needs:

TRAI's own enforcement and consumer engagement data demonstrates both scale and urgency. TRAI's annual enforcement update for 2025 indicates: over **31.09 lakh UCC complaints** were registered across channels, with **17.06 lakh** (over half) submitted through the DND application; and large-scale

action such as **7,31,120 notices** and **disconnection of 1,84,482 telecom resources** during 2025 for continued non-compliance. This supports a policy posture of stronger, faster enforcement while ensuring accuracy and redressal.

The direction dated 27 February 2026 on "AI/ML-based UCC_Detect intelligence" records that approximately **85% of UCC complaints** are against unregistered telemarketers (UTMs), and that subscriber-facing alerts without backend enforcement do not create deterrence—hence the need to institutionalize AI/ML outputs for coordinated action.

The draft consultation paper also recognizes a practical enforcement gap: AI-based detection deployed by major TSPs is used mainly to alert customers today, but does not itself cause deterrent action against UCC senders; the draft amendments aim to leverage AI/ML intelligence while corroborating with evidence and complaints to reduce false positives.

Spam and UCC are not only a nuisance; they are routinely used as vectors for fraud/impersonation and cybercrime. Public advisories by the Reserve Bank of India instruct consumers to report suspicious/fictitious offers and cyber-fraud promptly to law enforcement/cyber crime authorities. This broader harm profile supports a deterrence model that is responsive, evidence-led, and coordinated across stakeholders.

Legal grounding and regulatory coherence

The legal authority for making regulations is grounded in the Telecom Regulatory Authority of India Act, 1997, which empowers the Authority to

make regulations to carry out the purposes of the Act. The draft amendment notification itself cites issuance under section 36 read with clause (b)(v) and clause (c) of section 11(1).

Consumer consent and privacy principles should also be aligned with the Digital Personal Data Protection Act, 2023, which sets statutory requirements that consent be free, specific, informed, unambiguous, and that withdrawal be as easy as giving consent; it also contemplates proof obligations and structured consent management. These principles are directly relevant where the draft expands the concept of "Explicit Consent" to include legacy consents and requires subsequent registration in a consent register.

The draft also realigns certain definitions and references to the Telecommunications Act, 2023, including aligning "telecommunication" concepts and identifiers. The Telecommunications Act, 2023 itself contains an explicit "Protection of Users" chapter that contemplates prior consent for specified messages and maintenance of "Do Not Disturb" registers, and mechanisms to report contraventions. This makes it especially important that TCCCPR amendments reinforce a coherent "consent + DND + complaint + enforcement" chain rather than weaken it.

Where the draft proposes enforcement action relating to call management apps via the IT Act, 2000 and IT Rules, 2021, procedural clarity and inter-regulator coordination become essential—particularly in light of intermediary safe-harbour concepts (IT Act section 79) and the due diligence framework under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Finally, constitutional privacy norms recognized by the Supreme Court of India are relevant as a background principle: consumer control over personal information and communications constitutes a core element of informational privacy in India.

Comparative international practice and lessons relevant to TCCCPR

Global practice trends emphasize:

(i) consent/opt-out integrity,

(ii) strong enforcement,

(iii) call authentication and spoofing reduction, and

(iv) coherent complaint channels.

In the European Union, the ePrivacy Directive (Directive 2002/58/EC) establishes sector-specific privacy protections in electronic communications and includes specific rules for marketing communications. In the UK, the Information Commissioner's Office explains that PECR sits alongside the UK data protection framework and provides specific rules for marketing calls, texts, and emails. These frameworks underscore that marketing restrictions are privacy rules, not merely “nuisance” rules.

For SMS/email marketing compliance, Australia’s Spam Act framework—summarized in compliance guidance by the Australian Communications and Media Authority—emphasizes an easy and functional unsubscribe mechanism and clear sender information. Canada’s anti-spam approach, explained by the Canadian Radio-television and Telecommunications

Commission, similarly requires consent, identification, and unsubscribe mechanisms.

On robocalls and AI-generated voices, the Federal Communications Commission confirms that TCPA restrictions on artificial/prerecorded voice encompass AI technologies that generate human voices, and provides consumer-facing guidance on consent requirements for autodialed/prerecorded calls/texts. This is directly relevant to the draft's new "A2P call" definition and its focus on autodialling/robocalls/artificial voice.

For telemarketing do-not-call controls, the Personal Data Protection Commission outlines that DNC provisions generally prohibit organizations from sending marketing messages to numbers listed in the Do Not Call Registry (with consent-based exceptions).

Finally, to address "identity/spoofing" layers of unwanted calls, call authentication frameworks are a key global direction. The FCC describes STIR/SHAKEN as a caller-ID authentication approach to validate call handoffs and reduce spoofed robocalls. While TCCCPR is not itself a caller-authentication regulation, it should remain open to adopting technical standards/directions that enable verification of originating identity and classification, which strengthens both consumer trust and enforcement accuracy.

Comment Matrix in TRAI-prescribed Annexure format

This referral is not a substitute for the matrix below: the matrix is the formal submission.

The amendments are broadly directionally correct in focusing on A2P calling misuse, AI/ML-led detection institutionalization, and strengthening consumer appeals and evidence trails. The key risks to address through targeted edits are:

(i) consumer consent dilution via "legacy consent" recognition without strong notice/withdrawal flows,

(ii) AI false positives leading to disproportionate disruption,

(iii) compressing consumer complaint windows in a way that reduces redressal, and

(iv) definitions such as "on behalf of" creating loopholes for misuse.

Response matrix:

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
1	2	2(a) inserting clause (ea)	**1. Clarify and broaden A2P definition to capture "human-in-the-loop bulk dialer calls" and platform-mediated bulk calling**. Suggested drafting: after "without direct human dialling", add: "or where dialling is initiated, queued, or connected through automated/predictive dialer platforms at	1. The current definition focuses on calls initiated without direct human dialing and includes autodialling/robocalls/artificial voice. In practice, many scam and spam operations use hybrid dialers where agents speak but dialing and call distribution are automated; consumers experience the same nuisance and harm. A technology-neutral

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			scale, including human-agent bridged calls."	definition improves enforceability and prevents regulatory arbitrage by changing call initiation mechanics while maintaining spam scale. This aligns with international approaches that treat autodialed/prerecorded/artificial voice (including AI-generated voices) as regulated irrespective of superficial call-flow differences.
2	2	2(a) inserting clause (ea) "A2P call"	Expand A2P call definition to explicitly include **AI/GenAI conversational voice agents**, "human-in-the-loop predictive dialers," and "platform-orchestrated dialling" even where a human ultimately speaks. Suggested insertion after "without direct human dialling": "including calls where dialing, call distribution, call bridging, or first-response	The draft introduces A2P calls as "initiated by an application…including autodialling, robo-calls and/or prerecorded/artificial voice." Over 5–10 years, a large share of enterprise comms will be AI-assisted or bot-fronted (contact centers, reminders, authentication, conversational experiences). Without explicit inclusion, actors can evade compliance by labeling as "agent calls"

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			interaction is automated, including through conversational agents, synthetic voice, or predictive dialer systems."	while still automating dial/interaction. US regulators have clarified that AI-generated voices are "artificial" under anti-robocall frameworks—demonstrating that "synthetic voice" is recognized as a regulated risk surface. Impact: closes definitional loopholes, improves deterrence against future bot-driven spam/fraud; feasible via wording only.
3	2	2(b) substituting clause (y) "Explicit Consent"	**Add statutory consent quality attributes and proof burden**. Suggested addition to definition: "Consent shall be free, specific, informed, unambiguous, purpose-limited, time-bound where relevant, and recorded with auditable proof; the Sender shall be capable of proving consent in case of dispute."	DPDP Act requires consent to be free, specific, informed, unambiguous with clear affirmative action, and places proof obligations on the data fiduciary where consent is in question. The draft expands explicit consent to include verified consent recorded by consent registrar as well as verifiable means obtained outside CRF and subsequently registered. Without specifying quality and proof attributes, "verifiable means" can

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
				become a weak loophole. Aligning consent quality strengthens consumer privacy and reduces disputes and complaint reopening.
4	2	2(b) substituting clause (y) "Explicit Consent"	Add DPDP-aligned consent quality attributes and portability: "free, specific, informed, unambiguous, purpose-limited, revocable with equal ease; recorded in auditable form with proof burden on sender."	The draft broadened explicit consent to enable digitization of lawful legacy consents and business continuity, provided they are registered in Consent Register under Authority procedures. DPDP consent manager requirements emphasize accessible records of consents, notices, withdrawals, and sharing logs. Codifying consent quality future-proofs against consent fatigue and disputes, and enables interoperable consent in an omnichannel future (voice/SMS/RCS/OTT). Impact: stronger consumer control, reduced complaint closures based on consent ambiguity; feasible through definitional precision and CoP updates.
5	2	2(b) substituting	**Mandatory consumer**	The explanatory note

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
		clause (y) "Explicit Consent"	**"notice + easy revocation" when legacy consent is digitized**. Add proviso to definition: "Where consent is uploaded/registered from legacy/offline sources, the Recipient shall be notified (SMS/email/app) with details of Sender, purposes, and a one-step revocation method; unless the Recipient confirms/does not object within a defined period, such consent shall not be used for promotional communications."	explicitly states that the revised explicit consent definition is intended to recognize and digitize legacy consents while preserving subscriber rights to be notified and revoke consents. DPDP Act similarly requires informing data principals about pre-Act consent-based processing and ensures easy consent withdrawal. "Digitization without notice" risks mass misuse and could recreate the nuisance at scale while claiming historical consent. A notice-and-revocation flow is both pro-consumer and business-continuity-friendly.
6	2	2(b) "Explicit Consent" (new proviso)	Insert a **mandatory consumer notice and easy withdrawal** requirement for legacy consent migration: whenever legacy/offline consent is registered, the recipient must receive notice identifying sender, purposes, channels,	The consultation paper explicitly aims to recognize/digitize legacy consents while ensuring transparency and recipient rights. DPDP consent manager model requires logs and user access to consent records. A notice-and-revocation flow prevents "silent consent

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			and a one-step revocation method.	expansion," reduces consent fatigue, and aligns with global best practices against consent laundering. Singapore's DNC guidance treats consent acquisition itself as regulated to prevent bypass.
7	2	2(d) substituting "Regulatory Sandbox"	Add sandbox consumer safeguards: public scope/duration; eligible customer protection; opt-in/notice where consumer preferences may be affected; independent monitoring and exit criteria.	The draft defines regulatory sandbox and the consolidated regulation recognizes sandbox use for testing regulatory checks using DLT and complementary technological solutions. As networks evolve toward 6G and NTN integration, sandboxes become critical for testing new trust controls (caller authentication, consent APIs, fraud analytics). Safeguards ensure innovation does not externalize risk onto consumers.
8	2	2(e) substituting clause (bb) "Relationship"	**Support narrowing "Relationship"; add anti-misuse guardrails**. Suggested addition: "Relationship shall not	The draft narrows "Relationship" to business/commercial reasons and recent applications within three

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			be construed to permit Promotional messages/calls unless explicit consent exists; 'application' shall not include mere lead-generation forms without double-opt-in."	months. The explanatory note shows intent to prevent nuisance "in the name of inquiry" and to avoid misuse of inferred consent. To prevent new loopholes, the relationship concept must be explicitly bounded to service/transaction facilitation and not become a proxy for marketing without consent—consistent with consent-centric regimes internationally.
9	2	2(d) substituting clause (ba) "Regulatory Sandbox"	**Insert minimum consumer safeguards for sandbox relaxations**. Add at end: "Provided that any relaxation granted under sandbox shall be subject to (i) published scope and duration, (ii) explicit informed consent of participating customers where their communications preferences may be impacted, and (iii) independent monitoring and exit criteria."	The draft redefines sandbox as a live testing environment with limited eligible customers and certain relaxations to encourage innovation and refinement of codes of practice. The Telecommunications Act, 2023 also defines regulatory sandbox in similar terms. A telecom sandbox should not dilute consumer protections invisibly; safeguards maintain legitimacy and prevent consumer harm

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
				while still encouraging innovation.
10	2	2(c), 2(g), 2(h) (Telecom Act alignment)	**Support definitional alignment; add interpretive clause to avoid ambiguity**: "References to definitions under Telecommunications Act, 2023 shall be read as amended from time to time."	The draft replaces references to the Indian Telegraph Act with Telecommunications Act, 2023 and aligns "telegraph" to telecommunication equipment/identifier concepts. A standard interpretive clause prevents future ambiguity and strengthens legal coherence without changing consumer rights.
11	3	3(1) proviso (authority may classify senders)	Convert permissive classification into a **risk-based sender taxonomy** with published criteria and consequence bands: (i) Critical service verified, (ii) Regulated BFSI/health/education, (iii) High-volume CPaaS/aggregator-mediated, (iv) MSME/low-volume, (v) New/unknown risk. Require publication of classification parameters and	The draft already enables sender classification and later provides parameters (criticality, scale, regulatory status, impact on consumers). Over 5–10 years, enterprise comms will shift to CPaaS and automation; risk categorization is necessary to avoid "one size harms all" while still deterring abuse. Industry trust frameworks show supply-chain roles and codes of conduct spanning operators, aggregators,

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			periodic review.	cloud comms providers, and enterprises. Impact: fewer consumer disruptions from blunt actions; more targeted enforcement for high-risk sender types; feasible via Authority orders/CoP templates.
12	3	Regulation 3(1) proviso	**Support sender classification power; require transparency, consultation, and consumer non-regression**. Suggested drafting: "Any classification shall be published with reasons, and shall not reduce baseline consumer privacy/choice protections; differentiated enforcement shall be proportionate and ensure continuity of critical consumer services."	The draft proposes that the Authority may classify senders and specify different criteria for different classes. The explanatory note acknowledges that "one-size-fits-all" may not work and that enforcement against entities like banks could disrupt services. A transparent, proportionate approach ensures inclusion and service continuity while maintaining deterrence. This also aligns with proportionality factors present in user protection and penalty frameworks under Telecom Act 2023 (e.g., considering harm, repetition, mitigation).

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
13	4	Regulation 4 (substituted)	**Make A2P declaration operational and auditable via DLT**. Proposed addition: "Declaration shall be through DLT in a standardized format including: CLI range(s), purpose category, expected volume bands, and delivery entity/aggregator mapping; changes shall be updated within 24 hours."	The draft requires every sender to declare in advance to the OAP about use of A2P calls, and treats undeclared A2P calling as UCC. Without standardized, network-wide auditable declaration, enforcement risks being inconsistent and contestable. A DLT-based declaration flow builds evidence, reduces disputes, and supports inter-operator consistency (core to the TCCCPR architecture).
14	4	4 (A2P call intimation)	Require A2P declaration to be **DLT-recorded and standardized**, including: CLI range(s), enterprise identity, delivery platform/CPaaS chain, purpose category, expected volume bands, and a "verified caller policy compliance" flag.	Regulation 4 mandates prior declaration and treats undeclared A2P calls as UCC. A standardized DLT schema makes declaration auditable across operators and future-proofs against multi-platform orchestration. This increases enforceability and enables automation without sacrificing due process.
15	4	Regulation 4 (substituted)	**Make A2P declaration operational and auditable via DLT**.	The draft requires every sender to declare in advance to the OAP about

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			Proposed addition: "Declaration shall be through DLT in a standardized format including: CLI range(s), purpose category, expected volume bands, and delivery entity/aggregator mapping; changes shall be updated within 24 hours."	use of A2P calls, and treats undeclared A2P calling as UCC. Without standardized, network-wide auditable declaration, enforcement risks being inconsistent and contestable. A DLT-based declaration flow builds evidence, reduces disputes, and supports inter-operator consistency (core to the TCCCPR architecture).
16	4	Regulation 4 proviso	**Add aggravated consequence for "intentional non-declaration / misdeclaration"**. Suggested addition: "Repeated non-declaration or misdeclaration shall be treated as aggravated violation for penalty escalation under regulation 25/29."	The draft already treats undeclared A2P calls as UCC and requires action by OAP. A clear escalation path improves deterrence, particularly for bulk spam operators. This is supported by the explanatory rationale that A2P is misused due to cheap P2P routes and requires deterrent mechanisms.
17	11	Regulation 11(4) deletion phrase	**Clarify intent of deletion and ensure no enforcement weakening**: Add an explanatory clarification in regulation text or	The draft deletes specific words in regulation 11(4). Without clarity, removal could be interpreted as weakening interim containment measures

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			corresponding CoP that deletion does not eliminate ability to impose "usage caps" where proportionate and evidence-based against suspected spammers.	(usage caps) that can protect consumers while investigation proceeds. Given high volumes of complaints and persistent offenders, interim measures remain important so long as due process is preserved.
18	11	11(4) deletion ("usage cap…")	Reintroduce interim containment powers as a **time-bound, proportionate measure** with explicit due process: emergency "usage caps/temporary throttles" for suspected fraud/UCC bursts, with mandatory notice + review within fixed hours/days.	The draft deletes "usage cap" language. Future risk: scams and UCC bursts will be faster (automation, GenAI), requiring immediate containment. Safeguards should be explicit to prevent abuse. Due process is already reinforced in the draft via new appeals and representation mechanisms and audit CDR requirements.
19	21A	21A (AI/ML UCC_Detect actions)	Add **AI governance requirements**: minimum explainability categories in notices (without proprietary disclosure), human review gate before network-wide barring in borderline cases, model change management,	Regulation 21A operationalizes "Suspected UCC CLI" intelligence sharing and escalation; the TRAI direction explicitly states proprietary algorithms need not be disclosed. A governance layer is essential for long-term

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			and monthly reporting of false positive reversal rates to Authority.	legitimacy: future enterprise comms will look "bursty and automated" due to AI/CPaaS. Without governance, false positives can suppress legitimate services. Feasible: governance is reporting + procedural steps, not algorithm disclosure.
20	21A	21A(a)–(e) (new insertion)	**Support AI/ML institutionalization; require minimum "explainability without revealing proprietary algorithms"**. Add: "Notification to sender shall include CLI(s), time window, high-level trigger categories (volume/velocity/diversity anomalies), and a channel for timely representation."	The draft requires TAP to flag "Suspected UCC CLI" via AI/ML and share within two hours; and requires OAP to notify the sender. The 27 Feb 2026 direction explicitly states that nothing requires disclosure of proprietary algorithms/source code, while still mandating inter-operator sharing and notice. A "high-level reason" approach balances innovation/proprietary protection with procedural fairness and enables correction of false positives.
21	21A	21A(c)–(d) KYC identifier sharing	Add **data minimization and privacy safeguards**:	Regulation 21A requires identifying unique KYC identifiers and sharing via

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			pseudonymization/tokenization on DLT, limited access controls, and retention limits aligned to audit needs.	DLT across providers. DPDP consent manager standards include security safeguards, access control, and records; similar safeguards should apply to enforcement identifiers shared cross-network. This future-proofs against data misuse while retaining enforcement efficacy.
22	21A	21A(c) data sharing of unique KYC identifiers	**Insert data minimization and security language**: "KYC identifiers shared on DLT shall be restricted to what is necessary, pseudonymized where feasible, access-controlled, and retained only for defined periods aligned with investigation/audit needs."	The draft requires sharing unique KYC identifiers across access providers to identify all resources allotted to a sender. This is sensitive personal/company data; DPDP Act requires purpose limitation and structured governance for personal data processing, and also emphasizes language clarity and grievance mechanisms. Explicit privacy-by-design safeguards prevent misuse of enforcement data and improve trust.
23	21A	21A(e) thresholds and enforcement linkage	**Add a "false-positive safety valve" before network-wide barring**:	The draft triggers graded actions when five or more CLIs are flagged as

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			"Before barring outgoing services across all providers, OAP shall complete a quick human review and corroborate with complaint/traffic evidence; if evidence is insufficient, impose graded monitoring rather than barring."	suspected within ten days, including KYC reverification and potentially barring outgoing services for 15 days and subsequent escalations. The explanatory note itself emphasizes minimizing false positives by corroborating intelligence with evidence. Adding an explicit human review step strengthens accuracy without undermining enforcement speed.
24	22	22(1)(a) misuse of headers/templates	Add **"secure supply chain" obligations:** mandatory MFA for portal/API access; API key rotation; signed API requests; and "delivery entity chain logs" for CPaaS/aggregators, to support future enterprise automation.	Regulation 22 already mandates credential resets, LEA complaint filing, de-register/re-register on compromise, and monitoring of templates/headers. Over 5–10 years, enterprise comms will be API-first and automated; secure key management is essential to prevent "template hijack" and large-scale abuse. Implementable via CoP and audit.
25	22	Regulation 22(1)(a)(ii) security	**Mandate baseline credential/security**	The draft requires credential resets, law

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
		steps	**hardening**: add requirement for MFA for DLT/portal access, key rotation logs, and minimum cyber hygiene controls by sender/telemarketer/aggregator chains.	enforcement complaint filing, de-registration/re-registration after compromise, and review of all templates/consents. These steps are directionally correct; adding baseline MFA and audit log expectations reduces recurrent compromise events and supports consumer protection.
26	22	22(1)(a)(ii)(2) law enforcement complaint obligation	Add an optional **"central fraud reporting handoff"** mechanism: allow the OAP to file structured fraud indicator reports to designated cybercrime nodes for faster action, while retaining Sender's duty to file complaint.	Regulation 22 requires the sender to file a formal complaint identifying compromise cause and share a copy with OAP. Future risk is "attack speed"; structured reporting can reduce turnaround without removing sender accountability.
27	22	Regulation 22(1)(a)(i)–(iii) (misused headers/templates)	**Support targeted suspension approach; add "service continuity" carve-out for essential communications**: "Where Sender is a regulated entity providing critical	The draft shifts to immediate suspension of misused headers/templates, requiring notices and corrective actions, and escalates to broader suspension if non-compliance continues. The

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			consumer services, OAP may allow strictly transactional/government/service templates already verified, while misused promotional traffic remains suspended."	explanatory note acknowledges that blanket suspension for entities like government bodies/banks can disrupt services. A narrow continuity carve-out protects consumers who rely on essential alerts (fraud alerts, OTPs, service notices) while keeping deterrence against marketing misuse.
28	23	Regulation 23(1)(c) (consumer appeal)	**Support; add "reasoned speaking order" and "consumer evidence access"**: "Appellate Authority shall provide a reasoned decision and, on request, provide key evidence basis (CDR reference, template checks) subject to lawful limits."	The draft creates a consumer right to appeal within 15 days, requires disposal within 15 days, and requires a senior management-level appellate authority and publication of details. Many consumer grievances arise from complaints being closed with inadequate reasons; the explanatory note explicitly observes this and introduces appeals for accountability. A reasoned order strengthens transparency and auditability.
29	23	23(1)(c) consumer appeals	Add requirement for **reasoned speaking orders** and "key	Draft introduces consumer appeal within 15 days, disposal within 15 days,

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			evidence disclosure" (CDR match basis, template checks) subject to lawful constraints; require multi-language accessibility and parity of channels (IVRS/SMS/web/app).	and requires senior management appeal authority publication. Future consumer expectations demand transparency and accountability, especially where AI triggers action. OECD work on manipulative patterns supports a policy direction toward transparent and fair consumer choice and remedies.
30	23	Regulation 23(1)(c) appeal channels	**Explicitly require parity of channels with complaint channels**: incorporate into regulation text that all complaint modes (1909 IVRS/SMS/app/web/email) must also allow appeal initiation.	The draft already states that appeal should be possible through any mode specified for lodging complaint/report. To avoid implementation dilution, consumer parity across channels should be non-negotiable in both regulation text and CoP enforcement. This aligns with the Telecom Act user-protection orientation toward grievance mechanisms.
31	24	Regulation 24(3) complainant-wise history and evidence record	**Support 3-year records; add privacy safeguards and consumer access**	The draft expands records to include appeals and supporting documents for resolutions with 3-year

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			rights: "Access Providers shall protect records with appropriate security controls; consumers may obtain a summary of their complaint history upon request."	retention. This is essential for audit and accountability. At the same time, such records can contain personal data; DPDP requires privacy-by-design and grievance rights.
32	24	24(3) complaint/appeal record retention	Extend record retention to include **model/automation decision metadata** (decision rule category, timestamps, evidence pointers), enabling future auditability of AI enforcement.	Draft expands records to include appeals and supporting documents used to resolve complaints. As enforcement becomes more AI-enabled, auditability must include the decision context, not only the outcome. Feasible via structured logging.
33	25	Regulation 25(1) (DL-Complaints recording)	**Add "consumer correction window" for incomplete complaints**: before closure under 25(2), provide 24–48 hour window for consumer to correct missing details (auto-populated data editable in app/web).	The draft closes complaints where complete telephone number/header is unavailable and proposes educating the customer. TRAI's consumer reporting modes include app/web portals where extraction and editing of details can be designed for accuracy. A correction window reduces unjust closures and improves detection, consistent with accuracy-

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
				over-automation.
34	25	25(2) closure due to incomplete number/header	Add a **customer correction window** (24–48 hours) and permit TAP to auto-populate missing details (where available) to reduce unjust closures.	Draft closes complaints where complete telephone number/header is unavailable and "educates customer." With increasing reporting through apps/dialers, auto-capture of metadata is feasible; reduces consumer frustration and improves detection quality.
35	25	25(3) complaint window and "report" status	Future-proof by adopting a **15-day unified window** for complaint admissibility (not merely "report"), with a tiered evidentiary standard: older complaints may require stronger corroboration but still count for intelligence.	Draft retains 7-day complaint validity, converts later to "report," and mandates recording for reports up to 15 days. Over time, users will increasingly discover fraud later (multi-channel scams, delayed realization). A tiered evidentiary approach preserves fairness while keeping intelligence useful.
36	25	Regulation 25(3) (7-day complaint validity; 15-day recording)	**Pro-consumer modification: treat complaints reported within 15 days as "complaints" (not merely "reports") for enforcement thresholds, with clear evidence rules**.	Draft currently: complaints after 7 days are closed, changed to "report", but those between 7 and 15 days must still be recorded by TAP and OAP. Recording but stripping "complaint" status risks weakening consumer redressal and

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			Alternatively, extend "complaint" window to 15 days uniformly.	undercounting enforcement triggers, despite the same underlying harm. TRAI's own enforcement metrics show consumer reporting is central to identifying violators.
37	25	Regulation 25(4) registered senders: template categorization enforcement	**Strengthen deterrence against wrong-category misuse while protecting service continuity**: maintain template blacklisting, but require mandatory root-cause analysis and corrective controls for repeated miscategorization; for critical sector senders, allow limited continuity of transactional alerts while promotional content is halted.	The draft includes consequences where content templates are registered in wrong category, including blacklisting templates and suspension if five templates are blacklisted for wrong category (as referenced in the draft text and explanatory note). This is appropriate because miscategorization is a major channel of consumer harm and bypass of preferences. A tailored continuity approach preserves consumer-essential communications while punishing marketing misuse.
38	25	25(4)–(6) and escalation actions	Insert a proportionality test before network-wide barring/disconnection:	Draft already provides severe actions for repeated violations including barring/disconnection and

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			severity, repeat pattern, number of recipients, criticality of service, mitigation steps; require explicit documentation.	device blocking, but also acknowledges differentiated criteria via sender classification parameters. Proportionality is essential to avoid harming consumers dependent on critical services while maintaining deterrence.
39	25	Regulation 25(4)(f) and 25(6) (action thresholds; suspension/disconnection)	**Introduce structured proportionality factors for enforcement actions** (similar to Telecom Act penalty factors): require written consideration of (i) severity, (ii) number of consumers affected, (iii) repetition, (iv) mitigation steps, before "all resources across network" disconnection for critical entities.	Draft includes strong consequences: 15-day barring for first instance, one-year disconnection/blacklisting and device blocking for subsequent violations, with representation and appeal routes. The draft also contemplates classification of senders and differentiated criteria to avoid large-scale disruption to consumers. Formalizing proportionality factors strengthens fairness and reduces systemic risk. Telecom Act 2023 explicitly uses harm/repetition/mitigation factors in penalty assessments.
4	25	Regulation	**Support lower**	Draft lowers action trigger

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
0		25(5)(d)(i) lowered threshold when AI flags (UTMs)	**threshold with AI corroboration; add minimum "confidence + evidence" requirement and ex post review**: mandate periodic review of false-positive rates and restoration outcomes.	to 3 complaints in 10 days when AI indicates suspected UCC CLI; otherwise 5 complaints threshold. This is consistent with the 27 Feb 2026 direction and the draft's objective of leveraging AI outputs for deterrence. However, AI misuse or model drift can cause bias; metrics and review keep accuracy central.
41	26	Regulation 26(2A) (recording within 15 days)	**Support; add uniform reporting interoperability between operators and consumer visibility**: mandate a standardized dataset for "reports" to enable AI detect patterning and audit, and allow consumer to view status in-app/web.	Draft requires access providers to maintain record of every alleged violation reported within 15 days and record reports received from other terminating access providers. This strengthens evidence trails and is consistent with AI-led enforcement needs. Consumers should be able to track the status seamlessly, as TRAI's reporting channels increasingly rely on digital interfaces.
42	26	26(4A) CDR access for audit	Expand (4A) to explicitly cover **AI flagging audit**	Draft introduces CDR provision to Authority for

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			and false-positive examination, not only complaint closure.	auditing complaint handling. Over 5–10 years, credibility will depend on whether AI-triggered actions can be audited as fair and accurate.
43	26	Regulation 26(4A) (CDRs to Authority for audit)	**Support; add safeguards**: "CDR provision shall be for limited periods, purpose-limited to audit/investigation, with confidentiality and security controls."	The draft empowers audit by requiring requested CDRs to be provided to the Authority. This is essential given consumer dissatisfaction with unjustified complaint closures noted in explanatory note. Privacy safeguards ensure responsible handling of traffic data, consistent with Telecom Act concepts of traffic data and security governance.
44	27	27(heading & disincentives)	Add progressive disincentives for repeated systemic failures (e.g., wrong template categorization failures in a quarter) and require mandatory remediation plans.	Draft shifts accountability to access providers for failure to take action and imposes disincentives for headers/templates issues. Progressive escalation strengthens deterrence while focusing on systemic negligence rather than one-off mistakes.
45	27	Regulation 27(1) provisos (financial	**Support shifting accountability to the**	Draft imposes ₹1,000 per valid complaint on the

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
		disincentives for wrong header/template registration)	**registering Access Provider; strengthen deterrence with escalation for repeat registration errors**: add progressive disincentive multipliers for repeated violations in a quarter.	Access Provider that registered misused headers in violation; and similarly for wrong categorization of content templates (on OAP and/or registrar AP). This improves accountability distribution (reduces blame-shifting). Progressive escalation discourages systemic negligence without penalizing isolated errors unduly.
46	29	Regulation 29 heading and proviso (partial restoration; minimum charges)	**Support "restoration charge floor"; require transparency and MSME protection**: publish restoration charge methodology; allow structured payment plans for MSMEs conditioned on compliance remediation.	Draft extends representation rights to telemarketers and introduces a proviso that partial restoration charges cannot be less than half of full restoration charges. This is deterrent-positive. However, to avoid undue burden on small businesses and ensure fairness, charges should be transparent and predictable, and restoration should be tied to verifiable remediation.
47	29	Restoration process (representation to	Introduce MSME-sensitive remediation: allow	Draft explains restoration charges are intended as deterrence and adds

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
		Authority)	structured restoration plans (partial restoration tied to verified controls), while retaining deterrent floor charges.	minimum floor for partial restoration. A forward-looking approach avoids undue burden on small legitimate businesses while remaining firm on repeat abusers.
48	34A	Regulation 34A(1) (ban on tagging/blocking designated series)	**Support preventing blanket blocking that harms legitimate communications; explicitly preserve user-level control** by adding: "Nothing prevents users from individually blocking numbers; default/blanket tagging by app/provider for designated series is prohibited."	Draft prohibits call management applications from blanket tagging/blocking calls from designated commercial communication series and requires that they not treat such calls differently from genuine communications. The consolidated text also indicates consumers should have right to individually manage their own calls. This balances consumer choice (personal blocking) with systemic fairness (no app-level blanket blocking that can distort regulated number series).
49	34A	34A(1)–(4) call management apps	Add privacy and audit requirements: data minimization for reports, user notice/consent for forwarding reports, and	Draft mandates call management apps not blanket-block designated series, to forward spam/UCC reports to DND registry, and creates

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			an API standard for forwarding to DND registry; require periodic compliance audits.	enforcement linkage via IT Act/IT Rules with opportunity to represent. As apps become primary user interface, interoperability must be privacy-safe and auditable; DPDP principles reinforce secure processing and accountable record-keeping.
50	34A	Regulation 34A(2) (mandatory reporting to DND registry)	**Strongly support; add data protection & transparency**: require clear user notice that "report spam" will be transmitted to operators/DLT and specify minimum data fields and opt-out of sharing contact list.	Draft requires call management apps/phone dialers to send spam/UCC reports to the DND registry in formats prescribed by the Authority. This is essential to unify complaint intake and improve enforcement speed (explanatory note cites this). User transparency reduces privacy concerns and improves reporting integrity.
51	34A	Regulation 34A(4) (IT Act / IT Rules enforcement; due process)	**Support action against non-compliant apps; require regulator coordination and procedural safeguards**: specify coordination mechanism with	Draft allows warnings, declaration as non-compliant/violator, and initiation of action under IT Act/IT Rules; it also includes a "reasonable opportunity to represent." Given intermediary liability

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			relevant authorities and time-bound hearing/decision timelines.	frameworks under IT Act section 79 and MeitY's IT Rules, enforcement should be procedurally rigorous and coordinated.
52	35	Regulation 35 proviso change ("by or on behalf of")	**Add "authorization proof" requirement to avoid misuse**: insert: "Where communication is claimed to be made 'on behalf of' a government/authority, the entity shall be explicitly authorized in writing and registered/whitelisted on DLT; misuse shall attract aggravated penalties."	Draft changes "by or on the directions of" to "by or on behalf of." While intended to clarify agency arrangements, "on behalf of" can be exploited by private entities claiming government association, increasing consumer risk of impersonation scams. An authorization/whitelisting requirement supports both consumer trust and genuine government communication.
53	35	35 proviso change ("on behalf of")	Add explicit "authorization proof + DLT whitelisting" requirement for "on behalf of" communications to prevent future impersonation misuse.	Draft changes "by or on the directions of" to "by or on behalf of." Forward-looking risk: sophisticated fraud ecosystems will increasingly claim "government on behalf of" cover while spoofing identity chains; whitelisting and authorization proof is implementable and limits abuse.
5	35A	35A termination	Make termination	Draft allows termination

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
4		charge for A2P calls	charges conditional on compliance tier: lower/zero charge for verified designated series with attested identity; higher charge for undeclared/non-attested A2P calls (while maintaining cap). Require transparency and prohibit pass-through to consumers.	charge up to ₹0.05/min for A2P calls and exempts government/bodies/Authority-directed and designated commercial series use. A compliance-tiered structure incentivizes migration to "trusted calling," enabling innovation in A2P voice (authentication, reminders) while discouraging cheap abuse routes in the future.
55	35A	Regulation 35A proviso exemptions	**Support exemptions; tighten "agency authorized" controls**: require a published list/identifier of authorized agencies and mandatory use of designated number series for exempt communications.	Draft exempts government/constitutional bodies/Authority-authorized agencies and calls using designated commercial communication series (e.g., 140xx, 1600xx). Exemptions are justified for public interest alerts. [36] Tight controls prevent exemption misuse under "on behalf of" cover and improve consumer trust in government alerts.
56	35A	Regulation 35A(1) A2P termination charge	**Support termination charge as deterrent; add non-pass-through and transparency rule**:	Draft introduces termination charge up to ₹0.05 per minute for A2P calls. Explanatory note

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			require that OAP/TAP not levy such charges on consumers as separate line items, and that any pass-through to senders be transparent.	frames termination charge as deterrent due to bulk misuse of cheaper P2P routes. Consumer bills should not become opaque; deterrence should target bulk callers/senders.
57	Schedule-I	Item 1 proviso (verification/authentication methods)	**Support flexibility; mandate minimum standards and inclusion**: require that alternative verification methods be at least equivalent in assurance to biometric/physical verification, and be accessible for rural/underserved entities without excluding legitimate MSMEs.	Draft empowers Authority to prescribe other manners of verification/authentication. This is future-proofing. However, weaker KYC/verification will increase UCC and fraud risk; minimum assurance levels and inclusion guardrails protect consumers while not overburdening legitimate small businesses.
58	Schedule-I	Item 1 proviso (other verification/authentication methods)	Link alternative verification to **digital identity assurance levels** and fraud prevention signals (SIM change/port checks for high-risk onboarding), with a privacy-by-design requirement.	Draft allows Authority to prescribe other verification/authentication methods beyond physical/biometric. Over 10 years, remote onboarding, e-KYC evolution, and fraud risk require flexible methods—but with assurance levels and auditability.
5	Schedu	Item 4(3)(m)	**Strongly support; add**	Draft introduces primary

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
9	le-I	primary registration & secondary validation of templates	**dispute-resolution and timelines**: "Secondary validation shall be completed within a defined timeline (e.g., 2 business days) and any inter-operator disputes on categorization shall be escalated to a common committee/Authority direction."	registration by one access provider and secondary validation by others for service/transactional templates (limited to category verification, no extra paperwork for sender). This improves accountability and reduces wrong-category abuse that harms consumer preferences. Clear timelines/dispute handling prevents service delays and protects inclusion.
60	Schedule-I	Item 4(3)(m) primary registration & secondary validation	Expand secondary validation beyond "category check" to include future-proofed "risk labels" and supply-chain checks (aggregator/CPaaS mapping), with strict timelines to protect business continuity.	Draft introduces primary registration and secondary validation of content templates for service/transactional messages, limited in scope to verification of category. As comms supply chains deepen, risk labels and mapping enable faster takedown and fewer false positives without adding heavy burdens.
61	Schedule-II	Item 1(1), item 1(2) (BLOCK PROMO and UNBLOCK ALL)	**Support simplification; strengthen consumer "privacy by default"**: require that new subscribers be	Draft defines BLOCK PROMO and UNBLOCK processes and migrates existing FULLY BLOCK to BLOCK PROMO. A default

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
			defaulted to BLOCK PROMO unless explicit opt-in is provided; ensure confirmations and easy reversal in all major languages.	promotional opt-out reduces spam exposure for new users and aligns with consumer-first principles and global trends emphasizing consent/opt-out integrity.
62	Schedule-II	BLOCK PROMO migration and preference architecture	Add "privacy by default" controls: require clear, non-manipulative UI (no dark patterns), periodic preference review prompts, and "single-view dashboard" compatibility with consent managers.	Draft migrates FULLY BLOCK to BLOCK PROMO and defines preference codes, allowing Authority to add/remove categories. OECD work on dark commercial patterns supports policy action to prevent manipulative choice architectures; DPDP consent manager records support a future where consent and preferences are user-visible and portable.
63	Schedule-II	Item 1 notes / inclusion	**Mandate accessibility**: require IVRS and customer care DND preferences in regional languages; require offline assistance for users without smartphones; special provisions for persons with disabilities.	The TCCCPR ecosystem depends on consumers being able to register preferences and report spam through multiple channels including IVRS/SMS/apps/web. TRAI enforcement data shows increased adoption of DND app, but inclusion requires equal functionality for non-

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
				app users.
64	Schedule-IV	Item 1(4) notice to suspected senders	**Standardize notice contents and add "remedy pathway"**: ensure notice includes: reason category, time window, how to stop, and how to contest; require that repeated suspected status triggers KYC actions only after corroboration.	Draft substitutes Schedule-IV notice provision requiring access providers to intimate senders detected as suspected UCC senders and to refrain from sending UCC. Given the draft's larger reliance on AI/ML UCC_Detect, standard notice formats and contest pathways reduce errors and improve compliance incentives.
65	Additional (new)	New provision to be inserted (suggested)	**Public "UCC transparency reporting"**: require each access provider to publish monthly statistics including complaints received, actions taken, restoration outcomes, and false-positive reversal rates (in aggregated form).	Consumer trust depends on visible improvements and accountability. TRAI's enforcement metrics show scale and provide a baseline; ongoing transparency reporting would institutionalize performance monitoring and enable stakeholder oversight. The consolidated regulations already contemplate publication of monthly UCC complaint summaries by access providers. The suggested addition strengthens transparency and governance.

Sl. No	Regulation number	Sub-regulation/ item number	Modification proposed to the draft amendment	Reasons/ full justification for the proposed modifications
66	Additional (new)	New provision to be inserted (suggested)	**Centralized consumer consent dashboard interoperability**: mandate that consumers can view and revoke all consents (including legacy) via a unified interface (DLT/app/web), with revocation propagated across delivery entities.	DPDP Act emphasizes easy withdrawal and enables consent management through consent managers, and requires notice and proof obligations. The draft's expansion to legacy consents will be safer and more trusted if consumers can easily view/revoke in one place.
67	Additional (new)	New provision to be inserted (suggested)	**Call authentication roadmap**: include an enabling clause for adoption of caller authentication/verification standards (e.g., digital validation of caller identity) for commercial calling, with phased implementation.	Many UCC/fraud calls involve identity misuse/spoofing; caller authentication frameworks like STIR/SHAKEN are used internationally to reduce spoofed robocalls by validating call handoffs. An enabling clause helps future-proof telecom consumer protection without delaying current enforcement reforms.

Implementation safeguards and forward-looking policy suggestions:

The draft amendments already move toward AI-led detection, network-wide coordination, and stronger evidentiary trails (DLT complaint recording; CDR access for audit). To ensure these reforms deliver consumer outcomes without undermining innovation or legitimate business continuity, the following implementation safeguards are particularly important.

First, AI/ML-led enforcement should be governed through measurable accuracy and fairness. The 27 February 2026 direction explicitly permits protecting proprietary algorithms while still mandating inter-operator sharing and coordinated action. Regulators can therefore require: periodic independent audits (confidential), publication of aggregate false-positive reversal rates, and minimum "reason categories" in notices without demanding source code.

Second, consent integrity must be protected particularly for "legacy consent migration." The draft's rationale is business continuity and orderly migration. The DPDP Act provides a model: give effective notice about pre-existing consent use and ensure easy withdrawal comparable to the method of giving consent. Applying this as a telecom compliance standard is a pro-consumer safeguard that also reduces complaint disputes, because consent becomes evidentiary and revocable.

Third, inclusion requires that non-smartphone users remain protected. TRAI's own consumer reporting ecosystem includes SMS/IVRS and web portal routes. If the system becomes "app-first," rural and elderly consumers may face higher UCC exposure and lower complaint success, undermining equity.

Fourth, deterrence should target spammers and negligent actors, but not create systemic consumer harm through disruption of essential services. The draft already recognizes the need for differentiated approaches for enterprises whose disconnection could harm consumers and the economy. A transparent sender classification framework—paired with "targeted

restrictions + continuity for essential alerts"—best satisfies both deterrence and consumer welfare.

Ten-year foresight map:

A 10-year horizon suggests the regulatory system needs to be **channel-agnostic, identity-anchored, risk-scored, audited, and interoperable**, because the following "macro shifts" are already underway:

Foresight dimension	Near term (1–3 years)	Mid term (3–6 years)	Later term (6–10 years)	Why this matters for TCCCPR
Technology	AI/ML in telecom networks; automated fraud scoring; app-based dialing/reporting	GenAI voice agents, conversational bots, behavioral analytics; increased automation in enterprise comms	6G/IMT-2030 evolution with broader capabilities and "inclusive information society" design goals; convergence with sensing/edge	AI-enabled UCC enforceability must include **governance for model drift and false positives**; "synthetic voice" vishing creates future UCC/fraud overlaps.
Networks	5G expansion; enterprise voice over SIP/PRI and cloud telephony	NTN integration with terrestrial networks; broader edge computing in networks	6G era technical performance requirements and new radio interface evaluations	TCCCPR must stay workable for (a) satellite/NTN calling chains, (b) edge-based filtering, and (c) new "telecom identifiers" across architectures.
Industry	CPaaS-style orchestration of voice/SMS; A2P voice growth;	Conversational AI contact centers; omni-channel	Fully integrated "trusted comms"	The compliance object shifts from "a message" → "a comms workflow

Foresight dimension	Near term (1–3 years)	Mid term (3–6 years)	Later term (6–10 years)	Why this matters for TCCCPR
	enterprise messaging trust programs	enterprise comms; telecom-OTT adjacency	ecosystems spanning operators, apps, and identity layers	with identity, consent, and audit trails," requiring APIs, dashboards, and supply-chain accountability.
Consumer behavior	Higher awareness of spam; increasing reporting through dialers/apps; demand for control	Privacy expectations rise; consent fatigue; resistance to manipulative UI patterns	Strong expectation of explainable enforcement, transparent consent, and trustworthy "verified caller" indicators	Consent and opt-out models must be **low-friction and anti-dark-pattern**, avoiding "consent laundering" while preserving legitimate communications.
Regulatory evolution	Technology-led enforcement; inter-operator intelligence sharing; app ecosystem coordination	Risk-based regulation; sandboxes; interoperability requirements; auditability and accountability	Cross-sector regulatory convergence (telecom + data protection + cybercrime + consumer protection)	TCCCPR needs explicit **interoperability hooks** for consent managers, verified caller identity, and cross-regulator takedown cooperation.

Risks and opportunities:

The main opportunity is that the draft materially strengthens the enforcement "loop": AI/ML systems detect behavioral anomalies, DLT shares intelligence, KYC identifiers are correlated across access providers, and escalations culminate in barring/disconnection for repeated suspected UCC behavior—

while also building procedural pathways (representation, appeals) and auditable evidence (DL-Complaints; CDR access for audit).

The main medium-term risk is **trust collapse due to false positives or opaque automation**. The draft relies on AI/ML "behavioral parameters" without specifying a minimum governance layer (performance reporting, bias checks, human review gates, and model change control). Over the next 5–10 years, as enterprise comms become increasingly automated and multi-agent, this becomes a credibility issue for legitimate communications and for consumer wellbeing.

A second risk is **consent dilution through legacy consent migration**. The draft intentionally broadens "Explicit Consent" to recognize lawfully obtained legacy consents and supports digitization into the Consent Register to protect business continuity. However, future consumer expectations and DPDP consent manager design principles point toward a stronger standard: notice, easy withdrawal, clear logs, and machine-readable portability. If not designed as "privacy by default," legacy migration can produce consent fatigue and disputes.

A third strategic risk is **identity/impersonation escalation** driven by AI-voice cloning and caller-ID spoofing. Outside India, regulators have explicitly recognized AI-generated voices as falling under "artificial voice" robocall restrictions, and call authentication frameworks have been adopted to restore trust in calling line identity. TCCCPR's A2P voice focus will be more future-proof if it includes an enabling pathway toward caller authentication/verified identity for designated commercial calling.

Draft gaps and future-proofing principles

The draft has strong building blocks, but some gaps will likely matter more over 5–10 years than they appear today.

The draft introduces A2P calls and a termination charge regime, including exemptions for government and designated commercial series (140xx/1600xx). However, it does not yet tie A2P calling to a **verified caller identity trust layer** (authentication, attestation, chain-of-custody), which other jurisdictions use to reduce spoofing and scams, and which becomes more critical in a GenAI voice environment.

The draft allows the Authority to classify senders and even provides the parameters (criticality, scale, regulatory status, impact of suspension) for differentiated enforcement. But it does not yet define a structured risk taxonomy (e.g., “critical service verified,” “regulated BFSI,” “high-volume CPaaS,” “new MSME senders”), nor a consistent consequence matrix that avoids both over-enforcement and under-deterrence.

The draft includes a “Regulatory Sandbox” definition and acknowledges sandbox operations for testing regulatory checks using DLT and complementary technologies. Over a 10-year horizon, sandboxes will become essential for integrating consent managers, verified caller identity, behavioral fraud analytics, and interoperability—but will need consumer safeguards to avoid experimental externalities.

The draft adds obligations for call management applications to refrain from blanket blocking of designated series, to pass spam reports to DND registry

formats, and creates an enforcement pathway tied to IT Act/IT Rules with procedural safeguards. Over time, this will become a key interoperability bridge between operator enforcement and consumer reporting, so privacy, data minimization, and auditability should be explicit elements.

A future-proofing principle that appears only implicitly is **anti-dark-pattern consent and choice architecture**. Global consumer policy work recognizes manipulative ("dark") commercial patterns and associated harms; in telecom consent and preference design, this translates into minimizing consent fatigue and prohibiting coercive opt-ins.

Global benchmarks and lessons for India:

The following global approaches are relevant because they are implementable lessons on **consent, identity trust, and enforceability**:

The **EU ePrivacy Directive** anchors rules for privacy in electronic communications and restrictions on unsolicited communications in a rights-based framework; it reinforces that unsolicited marketing control is not only nuisance management but privacy governance.

The UK combines privacy-marketing governance through **Information Commissioner's Office (ICO)** guidance on PECR and telecom security/scam mitigation through **Ofcom** work on CLI authenticity and scam call reduction, including operational measures against spoofing from abroad.

The US approach, led by **Federal Communications Commission**, emphasizes call authentication and consumer controls against robocalls/robotexts, and has explicitly stated that AI-generated voices are

"artificial" under TCPA restrictions. This is a clear signal that voice cloning fraud is treated as within existing telecom consumer-protection doctrine.

Singapore's **Personal Data Protection Commission** operationalizes "clear and unambiguous consent" under the Do Not Call framework, including strong guidance that consent collection itself cannot circumvent DNC restrictions in prohibited ways—an important guardrail to prevent consent laundering.

Australia's **Australian Communications and Media Authority** compliance guidance is implementation-oriented: consent first, identify the sender, and make unsubscribe easy—reinforcing low-friction consumer control as a baseline expectation.

Canada's approach under CASL, summarized in **Canadian Radio-television and Telecommunications Commission** guidance, similarly centers consent, identification, and unsubscribe as enforceable pillars.

Industry self-regulatory trust frameworks like **Mobile Ecosystem Forum** "Trust in Enterprise Messaging" and its business SMS code of conduct illustrate how supply-chain accountability (operators, aggregators, cloud comms providers, enterprises) can be operationalized through best-practice standards and compliance committees—useful as a complement to regulation for fast-moving channels and vendor ecosystems.

India-specific consumer protection needs

India's telecom consumer protection needs, in a 10-year horizon, strongly align with:

(i) multilingual inclusion,

(ii) fraud-resilience, and

(iii) interoperable consent control.

The Telecommunications Act, 2023 explicitly permits user protection measures including prior consent for certain specified messages, maintenance of “Do Not Disturb” registers, and user mechanisms to report malware or specified messages received in contravention, as well as online grievance redressal. This provides a clear legal backbone for expanding TCCCPR’s future-proofed consent and reporting architectures.

The DPDP Act and notified consent-manager requirements emphasize that individuals should be able to manage, review, or withdraw consent via consent managers, with accessible records (including notices and sharing logs) and long-term record retention; this strongly supports a unified “consent dashboard” direction for commercial communications, reducing consent fatigue and dispute costs.

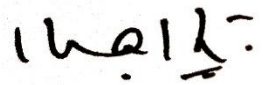
The draft itself already recognizes an ecosystem reality: consumer reporting often occurs through phone dialers/call management apps, and routing these reports into the operator DLT complaint systems accelerates identification and action against spammers. The same logic motivates building privacy-safe interoperability hooks so “reporting + consent + enforcement” can work across devices and across user literacy levels.

A final India-specific need is **digital inclusion by design**. The IMT-2030 framework explicitly positions future mobile communications development

toward inclusivity and bridging digital divides. TCCCPR's consumer control mechanisms should anticipate that meaningful connectivity and consumer protection must remain accessible even as networks evolve (5G/NTN/6G) and as the fraud landscape becomes AI-enabled.

Finally, call authentication should be treated as a forward roadmap, not an immediate blocker. Call authentication frameworks (e.g., STIR/SHAKEN) are globally positioned as anti-spoofing tools that support consumer trust in inbound calling identity. A roadmap clause within TCCCPR (or in parallel directions) can strengthen the future technical foundation for UCC enforcement, especially for A2P calling.

Thanks.



(Dr.Kashyapnath)
President