Luthra and Luthra
LAW OFFICES INDIA

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

JULY – SEPTEMBER 2024

INSIDE

In the **July – September 2024 edition** of the Luthra and Luthra Law Offices India – 'Technology, Media and Telecommunications ("**TMT**") Law Newsletter', we cover some of the most pertinent developments in the TMT law space over the last quarter.

This newsletter is only for general informational purposes, and nothing in this edition of newsletter could possibly constitute legal advice (which can only be given after being formally engaged and familiarizing ourselves with all the relevant facts).

FINTECH

1. Reserve Bank of India ("RBI") issues Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators ("PSOs")

On July 30, 2024, the RBI **issued** the Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators (**"Master Directions**") aimed at enhancing the security, resilience, and stability of the digital payment ecosystem. With the rapid growth of digital payments, the Master Directions are seen as a positive step towards mitigating risks, ensuring data privacy, and fostering a secure environment for financial transactions.

The Master Directions apply to all non-bank Payment System Operators ("**non-bank PSOs**") authorized by the RBI, mandating compliance across governance, security measures, and digital payment transaction protocols. For entities like payment gateways, third-party service providers, and vendors who operate in the PSOs' ecosystem, adherence to these Master Directions is required as per mutually agreed terms.

Regards practical enforcement, the Master Directions emphasise phased timelines for implementation:

- ***Large non-bank PSOs***: Compliance by April 1, 2025
- ***Medium non-bank PSOs***: Compliance by April 1, 2026
- ***Small non-bank PSOs***: Compliance by April 1, 2028 '

Further, the compliance obligations under the Master Directions are categorized into three key areas:

I. Governance Control Measures: Non-bank PSOs must develop a board-approved Information Security ("**IS**") policy, focusing on roles, responsibilities, and processes to assess and mitigate cybersecurity risks. A dedicated Chief Information Security Officer ("**CISO**") is required to oversee the implementation and continuous evaluation of the IS Policy and cyber-resilience framework. Regular board-level reviews and establishment of subcommittees are mandatory, with cyber risk assessment preceding any new product launch or infrastructure changes.

II. Baseline Information Security Measures/Controls: Comprehensive inventory management, network security, and access control protocols are emphasized. Key directives include:

- ***Access to Data***: Enforce stringent access controls, privilege limitations, and digital identity monitoring, ensuring that access to the IT environment is based on "need-to-know" principles.
- ***Vendor Risk Management***: PSOs must align with RBI's Framework for Outsourcing Payment and Settlement-related Activities and obtain independent assurance of vendors' cyber-resilience capabilities.
- ***Data Security***: Measures for data leak prevention, protection of Personally Identifiable Information ("**PII**"), and mandatory Payment Card Industry Data Security Standard ("**PCI-DSS**") certification – for card data storage are outlined.
- ***Incident Reporting***: Immediate notification protocols for cyber incidents to the RBI and to the Computer Emergency Response Team-In ("**CERT-In**") are required, with incidents like cyberattacks or fraud to be reported within 6 hours of detection.

III. Digital Payment Security Measures / Controls: PSOs must adopt secure messaging practices for sensitive information such as bank account or card numbers. Digital payment transactions must transparently display merchant details and amounts, and customers should have mechanisms to report fraudulent activity. Special controls for mobile, card, and Prepaid Payment Instrument **("PPI")** transactions are also detailed to enhance security.

The Master Directions come at a critical juncture, as India's non-bank PSOs play a significant role in expanding financial inclusion and digital payments. However, the proliferation of digital payment platforms has led to an increased vulnerability to cyber threats. By mandating robust governance, PSOs are better equipped to mitigate risks, instil consumer confidence, and align with international best practices.

However, it should be noted that the Master Directions introduce comprehensive changes that PSOs must implement, leading to an increase in operational and compliance costs. Implementing technology measures, ensuring vendor compliance, developing board-approved policies, and conducting frequent audits may require significant resource allocation whereby smaller PSOs might face challenges in meeting the financial and technical thresholds outlined under the Master Directions.

2. RBI Issues Draft Framework on Alternative Authentication Mechanisms for Digital Payment Transactions

RBI has recently released a draft "Framework on Alternative Authentication Mechanisms for Digital Payment Transactions" ("**Draft Framework**") to expand beyond short message service (SMS)-based One-Time Password ("**OTP**") authentication. The Draft Framework mandates for an Additional Factor of Authentication ("**AFA**") for digital transactions using cards, prepaid instruments, and mobile banking channels.

Some of the key principles for authentication as mandated under the Draft Framework are detailed below:

- ***Mandatory AFA***: Transactions require multiple factors for authentication.
- ***Different Factors of Authentication***: Issuers can choose from:
    - Knowledge-based (passwords/personal identification number (PINs)).
    - Possession-based (tokens/cards).
    - Biometric based (fingerprint/biometrics).
- ***Dynamic Authentication***: One factor must be dynamically created for each transaction i.e., the factor is generated after initiation of payment, is specific to the transaction and cannot be reused.
- ***Risk-based Approach***: Authentication depends on factors like customer risk profile, transaction value, and channel.
- ***Transaction Alerts & Consent***: Real-time alerts and explicit customer consent for new authentication mechanisms.
- ***Robust Technology & Vendor Neutrality***: Issuers must ensure robust technology and avoid exclusive third-party arrangements.

Further, under the Draft Framework, there lie exemptions from AFA for offline payments up to ₹500, contactless payments up to ₹5000, recurring transactions up to ₹1,00,000, FASTag, mass transit, and gift PPIs.

In toto, the Draft Framework recognizes the need for secure, frictionless payments in India's rapidly growing digital ecosystem. By introducing options beyond one-time password **("OTP")**-based authentication, the Draft Framework aims to align with technological advancements and evolving user behaviours. However, the challenge lies in balancing strong security measures with user convenience, particularly for small-scale transactions, where introducing additional steps may hinder the user experience.

Additionally, the Draft Framework also brings much-needed flexibility to the market, allowing PSOs and banks to implement technologies like biometric and behavioural authentication. However, the need for real-time transaction alerts, dynamic authentication, and transparent customer consent processes demands significant operational upgrades. Moreover, adopting multiple authentication factors and dynamic security mechanisms bolsters safety, but also brings concerns over data privacy, storage, and potential misuse. It remains to be seen how industry stakeholders ensure that new technologies adhere to robust data security protocols.

3. RBI Issues Draft Directions for Due Diligence of Touchpoint Operators in the Aadhaar Enabled Payment System (AePS)

On July 31, 2024, RBI released the 'Draft Directions for Due Diligence in the Aadhaar Enabled Payment System' ("**Aadhar Directions**"). to enhance the security of Aadhaar Enabled Payment System ("**AePS**") transactions, addressing the increasing incidence of frauds due to identity theft and compromised customer credentials. The Aadhar Directions outline both the onboarding process for AePS touchpoint operators and ongoing monitoring requirements to mitigate fraud risks, particularly in rural and semi-urban regions.

The AePS, operated by the National Payments Corporation of India ("**NPCI**"), allows basic banking transactions through biometric or OTP-based Aadhaar authentication. Touchpoint operators act as agents for acquiring banks, facilitating essential services like cash deposits, withdrawals, balance inquiries, and fund transfers. Given their crucial role, the Aadhar Directions seek to enhance the integrity of these operators' activities.

Certain key features of the Aadhar Directions are envisaged below:

- ***Onboarding of Touchpoint Operators***:

The Aadhar Directions prescribe a thorough onboarding process:

  - **Single Acquiring Bank**: Each AePS touchpoint operator must be onboarded by one acquiring bank, enhancing oversight and accountability.
  - **KYC Procedures**: Touchpoint operators inactive for over six months must undergo Know Your Customer ("**KYC**") updates before resuming operations, in line with the RBI's Master Directions on KYC, 2016.

- ***Ongoing Monitoring and Due Diligence***:

Acquiring banks are responsible for continuously monitoring touchpoint operators' activities:

  - **Transaction Limits**: Limits must be set based on the operator's risk profile.
  - **Geographical Consistency**: The operator's transactions should align with their registered location and risk profile.
  - **Risk-Based Controls**: Regular checks and adherence to NPCI regulations are mandated to ensure compliance and detect anomalies.

- ***Enhanced Security Measures and Guidelines Compliance***:

To protect the interests of consumers, all system participants must adhere to NPCI's rules and regulations governing AePS operations. Banks and the NPCI have been given three months to comply with the Aadhar Directions once issued in final form.

The Aadhar Directions aim to bolster security and trust within India's digital payment ecosystem. By tightening KYC norms and requiring real-time monitoring, the RBI seeks to mitigate fraud and identity theft risks, particularly benefiting rural and semi-urban users who rely on AePS. The single-bank onboarding simplifies oversight, streamlining operational processes and enhancing financial inclusion. While these measures are set to build greater confidence in digital payments, they also emphasize the need for risk management and compliance with NPCI regulations.

---

4. Other Fintech Updates

- **RBI issued a revised set of directions amending the Non-Banking Financial Companies — Peer-to-Peer Lending Platforms** ("**NBFC-P2P**") **Directions,** 2017, on August 16 and September 9, 2024, introducing several significant changes to enhance operational transparency, safeguard lender and borrower interests, and address compliance issues faced by the sector, reflecting RBI's intent to reinforce NBFC-P2P platforms as intermediaries rather than investment products, mitigating risks and promoting transparency.

IT AND DATA PROTECTION

1. Securities and Exchange Board of India ("SEBI") issued a circular envisaging a Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities

On August 20, 2024, SEBI enacted a comprehensive **Cybersecurity and Cyber Resilience Framework** (**"CSCR Framework**"), targeting all SEBI Regulated Entities ("**REs**"). This pivotal update aims to fortify the cybersecurity infrastructure amidst escalating cyber threats tied to the increasing reliance on digital platforms.

Certain key features of the CSCR Framework have been discussed below:

- ***Applicability***: CSCR Framework applies to a wide array of entities including, but not limited to, Alternative Investment Funds ("**AIFs**"), KYC Registration Agencies, Mutual Funds, Asset Management Companies, Portfolio Managers, Venture Capital Funds, Stock Exchanges etc.
- ***Mandatory and Recommendatory Guidelines***: CSCR Framework introduces a mix of mandatory and recommendatory cybersecurity practices that all listed REs must adopt. These include enhanced data protection measures, rigorous audit requirements, and advanced incident management protocols.
- ***Risk Assessment and Categorization***: Entities are classified into five distinct categories based on their size and the volume of transactions they handle, as specified in Annexure III to the CSCR Framework. This categorization dictates the specific cybersecurity protocols each entity must follow, ensuring a tailored approach to risk management.
- ***Information Technology ("IT") Governance and Compliance Oversight***: A critical component of the CSCR Framework is the establishment of an IT Committee for significant REs, including Market Infrastructure Institutions and Qualified REs. This committee, which must include at least one external cybersecurity expert, will oversee the adoption and enforcement of the Framework.
- ***Audit and Certification Requirements***: CSCR Framework mandates regular cybersecurity audits, Vulnerability Assessment & Penetration Testing **("VAPT"),** ISO certification, and other rigorous checks to maintain high security and resilience standards.

- ***Enhanced Focus on Third-party Risk Management***: CSCR Framework places substantial emphasis on managing risks associated with third-party service providers, requiring REs to enforce strict compliance and audit trails to mitigate potential vulnerabilities in their extended networks.
- ***Timeline for Implementation*:** The CSCR Framework mandates phased implementation deadlines to ensure entities are adequately prepared:
    - ***For Entities with Existing Circulars:*** The framework becomes effective on January 01, 2025.
    - ***For Entities New to the CSCR Framework*:** These entities have until April 01, 2025, to comply.

REs should prioritize the integration of the CSCR Framework's requirements into their operational and IT strategies. Investments in cybersecurity technologies, training for personnel, and strengthened internal and external audit mechanisms are crucial. Additionally, REs must establish clear channels of communication with all stakeholders to facilitate seamless adherence to the CSCR Framework.

2. Ministry of Electronics and Information Technology ("MeitY") issues Advisory for Swift Takedown of Prohibited Content from Online Platforms

On September 3, 2024, MeitY issued an **advisory** ("**Sep 3 - Advisory**") to intermediaries to promptly remove prohibited content from their platforms, urging intermediaries to complete the takedown process as soon as required, without waiting for the timeframes prescribed under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules 2021**"), and act proactively at the earliest opportunity.

This Sep 3- Advisory was issued with reference to the Bombay High Court ("**Bombay HC**") **order** in *National Stock Exchange of India Ltd. vs. Meta Platforms, Inc.* ("**NSE vs. Meta**"), where the Bombay HC directed Meta Platforms and other defendants to take down unauthorized content within ten hours of receiving a complaint from the NSE.

Delving into the background of the case, NSE had filed an urgent application against Meta (which operates Facebook and WhatsApp) and other defendants, including Telegram, to take down:

- Unauthorized, AI-generated videos of the NSE's Managing Director and CEO.
- Content misusing the NSE's trademark.

NSE emphasized that the grievance redressal mechanism for content removal is often slow and impractical for time-sensitive financial matters, leading to potential harm if fake videos circulate unchecked. The urgency of market-sensitive information demands immediate action to prevent investors from being misled.

The Bombay HC held that intermediaries must exercise due diligence as per Rule 3(1) of the IT Rules 2021, making reasonable efforts to remove prohibited content upon receiving complaints. The HC provided interim relief, ordering the defendants to remove objectionable content within ten (not exceeding fourteen) hours from receiving a complaint from NSE.

Following the Sep 3-Advisory, MeitY issued a **further advisory** on September 13, 2024 ("**Sep 13- Advisory**"), advising significant social media intermediaries ("**SSMIs**") to ensure:

- Accountability towards creating an open, secure, and trusted internet.
- Compliance with obligations applicable to SSMIs, including publishing periodic compliance reports detailing complaints received, actions taken, and the number of removed or disabled links through proactive monitoring.

It is pertinent to note that the Bombay HC's directive is limited to specific intermediaries (Meta and others involved in this case) to address content flagged by a specific complainant (the NSE) through a designated email. This aligns with the obligation to promptly take down content that is of a sexual or impersonation nature, bypassing detailed adjudication. The ten-hour timeline is an ad-interim measure, reflecting the urgency of the case, rather than a general rule for all intermediaries.

3. Bombay HC Strikes Down IT Rules 2021 on Fact-Checking Unit

On September 20, 2024, the Bombay High Court delivered a landmark decision in the case of *Kunal Kamra v Union of India*, which challenged the constitutionality of certain provisions within the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2023 **("IT Amendment 2023").** Specifically, the

Bombay HC struck down Rule 3(i) (II)(A) and (C) **("Disputed rules")** of the IT Amendment 2023 which amended Rule 3(1)(b)(v) of the IT Rules 2021.

Delving into the background of the case, the Central Government had empowered the MeitY to establish a Fact Check Unit ("**FCU**") tasked with identifying and mandating the takedown of content considered fake or misleading regarding government activities on various digital platforms. The failure of intermediaries to comply with this obligation would lead to the loss of their safe harbour protection under Section 79 of the Information Technology Act, 2000 **("IT Act").** This authority of the FCU was challenged for violating fundamental rights such as free speech and equality under the Indian Constitution.

The key findings by the Bombay HC have been discussed below:

- ***Free Speech Implications***: The Disputed rules imposed restrictions on free speech that were not "reasonable" within the context of Article 19(2) of the Indian Constitution. It was determined that the State does not have the prerogative to decide the truthfulness of information, and such a mandate could lead to excessive censorship and self-regulation among content creators and intermediaries.
- ***Vagueness and Arbitrary Enforcement***: The Disputed rules were criticized for its vague definitions of what constitutes "fake, false, or misleading" information. Such ambiguity could lead to arbitrary enforcement by the FCU, which could act without a clear standard, thereby infringing on Article 14 of the Indian Constitution that guarantees equality before the law.
- ***Excessive Delegation of Power***: The Bombay HC highlighted that the delegation of such sweeping powers to the FCU without clear guidelines or legislative backing was an excessive and improper delegation by the legislature.
- ***Violation of Equality Under Law***: The distinction created between digital media and other forms of media (like print and broadcast), and between information concerning government business versus other types, was deemed discriminatory and unjustifiable under Article 14 of the Indian Constitution.

This judgment is pivotal in addressing the balance between regulating digital content to prevent misinformation and protecting constitutional rights such as free speech and equality. The ruling emphasizes that while regulating misinformation is a valid

government goal, it must not infringe upon fundamental rights or grant unchecked power to any government entity.

---

4. Other IT and Data Protection Updates

- **Government unveils Vishvasya-Blockchain Technology Stack, a National Blockchain Framework to bolster Digital Trust and Governance in September 2024,** in order to offer Blockchain-as-a-Service ("**BaaS**") through a distributed infrastructure hosted at NIC data centers in Bhubaneswar, Pune, and Hyderabad. This launch includes 'NBFLite' (a sandbox for startups/academia), 'Praamaanik' (for mobile app verification), and the 'National Blockchain Portal' as part of the National Blockchain Framework.

- **SEBI penalizes NSE Data and Analytics Ltd., a 100% step-down subsidiary of NSE Ltd, for cybersecurity non-compliance,** in an order outlining a range of infractions including irregularities concerning the business continuity plan/disaster recovery policy of the intermediary, delays in dispatching acknowledgment letters and anomalies in system audit reports and the cybersecurity audit framework. Notable among the violations was the failure to close VAPT activities within prescribed timelines which was not properly documented in the cybersecurity audit reports and omissions of essential clauses including reporting mechanisms for cyber-attacks, threats, cyber incidents, and breaches, as well as clauses regarding the periodicity of conducting cybersecurity audits.

TELECOMMUNICATIONS

1. Telecom Regulatory Authority of India ("TRAI") notified amendments to the regulatory framework for broadcasting and cable services

On July 8, 2024, the TRAI **released a series of amendments** aimed at simplifying the regulatory framework for broadcasting and cable services. These amendments, along with new recommendations to the Ministry of Information and Broadcasting ("**MIB**") regarding the listing of channels in the Electronic Programme Guide ("**EPG**") and transitioning DD Free Dish (a free-to-air satellite television provider owned and operated by Public Service Broadcaster Prasar Bharati) to an addressable system, are part of an effort to facilitate sectoral growth, promote transparency, and improve consumer protection.

The amendments to the regulatory framework are the culmination of several years of consultations with stakeholders. TRAI had released a consultation paper in August 2023 to gather industry input on various matters like pricing, channel listings, operational protocols, and the competitiveness of the broadcasting and cable sector. Based on feedback, TRAI recognized a need for flexibility to adapt to evolving market conditions and to foster a competitive environment while safeguarding consumer interests.

Certain key changes to the regulatory framework have been envisaged below:

- ***Network Capacity Fee ("NCF") Ceilings Removed*:** One of the major changes introduced by TRAI is the removal of ceilings on the NCF. Previously, the NCF was capped at ₹130 for up to 200 channels and ₹160 for more than 200 channels. With this change, Distribution Platform Operators ("**DPOs**") have the flexibility to set NCF based on factors like the number of channels offered, regional considerations, and customer classifications.
- ***Increased Discounts on Channel Bouquets*:** To enhance consumer choice and promote flexibility, TRAI has increased the maximum permissible discount that DPOs can offer on channel bouquets from 15% to 45%. This provides DPOs greater flexibility in forming channel bundles and creating more attractive subscription packages for consumers.
- ***Pay Channels on Public Platforms to be Free-to-Air*:** Any pay channel that is offered without a subscription fee on a DTH platform run by a public service broadcaster must now be declared free-to-air across all addressable platforms.

- ***Simplified Carriage Fee Regime*:** To further promote high-definition ("**HD**") content and simplify regulatory compliance, TRAI has removed the distinction between HD and standard-definition ("**SD**") channels for carriage fee calculation. Under the new rules, DPOs will have the option to charge a single, unified carriage fee, simplifying the structure and promoting ease of business.

Apart from the above, there are certain other revisions carried out to the Quality of Service **("QoS")** Regulations delineated in brief below:

- ***Display of Tariff Information in EPG*:** DPOs are required to display both Distributor Retail Price ("**DRP**") and Maximum Retail Price ("**MRP**") for channels in the EPG, thereby enhancing transparency and enabling consumers to make informed decisions.
- ***Financial Disincentives and Compliance Measures*:** TRAI has introduced financial penalties for violations of the Tariff Order and key provisions of the interconnection and QoS regulations.

These regulatory amendments come amid ongoing concerns from stakeholders like cable operators and DPOs, who have expressed concern over perceived regulatory imbalances. Concerns have also been raised about the advantage that public platforms have over private DPOs due to their differing regulatory burdens. This updated framework by TRAI aims to address some of these concerns by establishing a level playing field, reducing compliance complexities, and promoting transparency, all while ensuring that consumer interests remain protected. By enhancing the sector's operational dynamics and enabling market-driven strategies, these amendments are expected to catalyse growth in India's broadcasting and cable services sector.

2. Department of Telecommunications ("DoT") releases four sets of draft rules covering interception, internet suspension, telecom cybersecurity, critical telecom infrastructure for consultation.

The DoT has recently released four draft rules **("Draft Rules")** under the Telecommunications Act, 2023 ("**Telecom Act**") for public consultation covering aspects ranging from **temporary suspension of telecommunication services** to **lawful interception**, **cybersecurity,** and **critical infrastructure** with the objective to operationalize certain provisions of the Telecom Act, which was notified on December 24, 2023, and is set to be enforced in a phased manner.

The four Draft Rules have been discussed below:

1. ***Temporary Suspension of Telecommunication Services Rules, 2024:*** The Draft Rules aim to replace the existing Temporary Suspension of Telecom Services Rules, 2017, issued under the Indian Telegraph Act, 1885. The provisions largely mirror the current rules, allowing central or state authorities to suspend telecommunication services for up to 15 days during public emergencies or for safety concerns. Suspension orders must specify the geographical extent, duration, and reasons for the shutdown. However, the prescribed 15-day period seems excessive for such orders, as these situations are typically exceptional and may require only short-term measures of 1 to 3 days. Furthermore, while the review committee retains executive control, its composition and structure raise concerns about lack of transparency and effective oversight.
2. ***Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024:*** The Draft Rules primarily retain the structure of existing rules under the Telegraph Act 1885 for lawful interception. A key change is the inclusion of entities establishing or maintaining telecom networks, such as satellite or terrestrial networks, which are now required to comply with interception orders. Moreover, the Draft Rules introduces provisions for lawful interception testing and monitoring facilities, which is a significant addition. However, the term "lawful interception systems" remains undefined, potentially broadening the scope of interpretation. The ambiguity raises uncertainty about the inclusion of over-the-top **("OTT")** communication services, such as WhatsApp and iMessage, within the ambit of interception rules, raising significant regulatory and privacy concerns.
3. ***Telecommunications (Telecom Cyber Security) Rules, 2024:*** The Draft Rules seek to replace the Mobile Device Equipment Identification Number Rules of 2017. They empower the central government to seek traffic data or any other relevant data from telecom entities for cybersecurity purposes. Moreover, telecom entities are mandated to adopt cybersecurity policies, conduct regular audits, establish Security Operations Centres, and report security incidents within six hours to the Central Government. All mobile devices must have their International Mobile Equipment Identity ("**IMEI**") numbers registered, and tampering with IMEI numbers will lead to the devices being blocked from accessing networks. The inclusion of a requirement for a Chief Telecommunications Security Officer ("**CTSO**") and adherence to cybersecurity policies indicates a push towards tightening security and addressing cyber threats more effectively.

4. ***Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024:*** Introducing the concept of Critical Telecommunication Infrastructure ("**CTIs"**), the Draft Rules define CTIs as telecom networks that, if disrupted, could severely impact national security, economy, or public safety. The Draft Rules authorize the Central Government to inspect the software and hardware of CTIs, access network details, and review the Cyber Crisis Management Plans. Telecom entities are obliged to implement stringent security measures, maintain records, and disclose any security incidents within two hours. The CTSO will be responsible for ensuring compliance with these Draft Rules.

The Draft Rules introduced by the DoT reflect an ambitious effort to enhance regulatory clarity, but several areas demand deeper analysis. Firstly, while the public consultation process is a welcome step, there is a clear need for a provision within the Telecom Act mandating such consultations before rule finalizations. A mandatory periodic review of regulations could ensure that they remain relevant and adaptable to technological and market changes. The applicability of these rules to OTT communication services, like WhatsApp and iMessage, is ambiguous, leading to significant regulatory uncertainty and privacy concerns.

Moreover, the executive-led review mechanism for interception and suspension lacks the independent oversight necessary for fair scrutiny, potentially allowing overreach without judicial or parliamentary checks. The 2018 Srikrishna Committee Report notably criticized this review system for being overwhelmed by high volumes of orders, thereby reducing its effectiveness. Also, broad and undefined provisions, particularly regarding "traffic data" access for cybersecurity, may lead to overly invasive practices, risking user privacy and data security. Finally, while the emphasis on cybersecurity is commendable, the lack of specific standards and enforcement guidelines highlights a need for more detailed provisions to ensure compliance and safeguard user rights effectively.

3. TRAI issues Directive for Access Providers to Disconnect Resources and Blacklist Unregistered Telemarketers for Spam Calls

On August 13, 2024, TRAI **issued a directive** **("Directive")** to all Access Providers to disconnect telecom resources of unregistered senders, referred to as Unregistered Telemarketers ("**UTMs**"), involved in sending unsolicited commercial communications, as per the Telecom Commercial Communications Customer Preference Regulations, 2018 ("**TCCCPR**").

The key features of the Directive are envisaged below:

1. ***Immediate Stoppage of Unregistered Telemarketing***: All Access Providers are required to stop promotional voice calls from UTMs immediately.
2. ***Disconnection and Blacklisting***: If any UTM is found to be misusing telecom resources for commercial voice calls, all telecom resources allocated to them by the Originating Access Provider ("**OAP**") must be disconnected for up to two years, and they must be blacklisted for the same duration.
3. ***Sharing of Blacklist Information***: Once a sender is blacklisted, the OAP must share this information with all other access providers on the Distributed Ledger Technology ("**DLT**") platform within 24 hours. The other Access Providers are then required to disconnect their resources to that sender within the next 24 hours.
4. ***Prohibition of New Allocations***: No Access Provider shall allocate new telecom resources to any sender who has been blacklisted during the period of their blacklisting.
5. ***Migration to DLT Platform***: All unregistered senders using telecom resources to make commercial voice calls must be migrated to the DLT platform within one month of the directive.

TRAI's actions come in response to over 12 lakh complaints against UTMs in 2023 and 7.9 lakh complaints in the first half of 2024. It was observed that while access providers disconnected specific resources of offenders, the offenders often continued spam activities using other telecom resources. Regards, reporting and compliance, access providers are required update their internal Code of Practice (CoP) accordingly; report the status of actions taken against UTMs within 15 days of the directive's issuance and submit bi-monthly reports on actions taken against UTMs on the 1st and 16th of each month.

This move by TRAI aims to curb spam calls, ensure effective action against repeat offenders, and protect consumers from the increasing menace of unsolicited commercial communications.

4. TRAI issues Directives to Access Providers to regarding measures to curb misuse of Headers and Content Templates under TCCCPR, 2018

On August 20, 2024, TRAI **issued directions** to address fraudulent activities conducted through commercial messages, particularly those of a promotional and transactional

nature. Some aspects of these directions were later revised on August 30, 2024, allowing additional time for certain compliances ("**Revised Directions**"). These measures, when read together, continued TRAI's recent efforts to curb unsolicited commercial communications ("**UCC**"), as governed under the TCCCPR.

Despite the implementation of TCCCPR to regulate commercial communications using telecom resources, such as SMS and phone calls, TRAI observed that registered Headers and Content Templates were being misused to fraudulently deceive the public. Under the TCCCPR framework, commercial messages were supposed to use registered headers (for sender identification) and content templates (for both transactional and service messages) assigned to specific senders (Senders). However, several malpractices were noted, such as unauthorized use of headers, the use of misleading terms like "disconnections," "lottery," and "OTP" in content templates, and the inclusion of malicious URLs or APKs. Additionally, some promotional messages were incorrectly categorized as service or transactional messages, leading to fraudulent activities.

To resolve these issues and enhance message traceability, previously, TRAI had released several directives which, as observed, were not fully implemented by Access Providers.

Key actions included:

- ***February 16, 2023***: Directed Access Providers to reverify all headers registered on the DLT platform, block unverified templates, and establish the complete chain of telemarketers engaged by the Principal Entity to improve message traceability.
- ***May 12, 2023***: Mandated Access Providers to ensure that only whitelisted URLs, APKs, OTT links, and call-back numbers were included in message templates.
- ***May 4, 2024***: Directed Access Providers to implement DLT-based voice solutions for messages using the 140-numbering series.
- ***March 22, 2024***: Issued a directive to resolve look-alike headers to prevent potential misuse and fraud.

To build on these earlier initiatives, TRAI has issued the following key directives:

- ***Implementation of 140-numbering Series***: Access Providers were directed to ensure end-to-end implementation of the 140-numbering series on the DLT platform by September 30, 2024, for enhanced monitoring and control.

- ***Whitelisted URLs and Links***: Access Providers were prohibited from transmitting messages containing URLs, APKs, or OTT links that were not whitelisted by Senders, effective October 1, 2024 (as per the Revised Directions).
- ***Enhanced Message Traceability***: Access Providers were required to ensure traceability of messages from Principal Entities to recipients starting November 1, 2024, rejecting messages with undefined or mismatched telemarketer chains.
- ***Blacklisting Misclassified Content Templates***: In cases where content templates were registered under the wrong category (e.g., promotional content misclassified as service messages), those templates were to be blacklisted. Should five templates be blacklisted, the Originating Access Provider was required to suspend the Sender's services for one month or until templates were reverified.
- ***One Header per Template***: To prevent misuse, content templates were required to be linked to only one header. In instances of misuse by another entity, all Access Providers were to immediately suspend traffic from the Sender until corrective measures were taken or a complaint/FIR was filed. Similarly, if a delivery telemarketer misused headers or content templates, Access Providers were to take swift action to trace and block the offending entity.

The rise in fraudulent commercial messages necessitated a strong regulatory approach, and TRAI's Revised Directions are aimed at mitigating such risks by mandating the use of whitelisted URLs and enhancing message traceability. The blacklisting of miscategorized content templates and the suspension of services for repeat offenders are steps aimed at deterring social miscreants. The Revised Directions, in essence, create a secure ecosystem for consumers by issuing specific directives with stringent timelines. However, the success of the Revised Directions depends on strict compliance by Access Providers. There has also been a possibility of disruptions in the delivery of some transactional and service messages during the realignment process, potentially causing inconvenience to consumers.

5. Department of Telecommunications (DoT) Notifies the Telecommunication Right of Way Rules, 2024

On September 19, 2024, the DoT **notified the Telecommunications Right of Way Rules, 2024** (the "**RoW Rules**") which supersede the Indian Telegraph Right of Way Rules, 2016, and the Indian Telegraph (Infrastructure Safety) Rules, 2022, notified under the Indian Telegraph Act, 1885.

Key highlights of the RoW Rules have been discussed below:

- ***Applicability and Application Process***: The RoW Rules apply to all instances where right of way is required for telecommunication infrastructure on public or private property. To ensure transparency, all right of way applications must be submitted through a designated online portal.
- ***Appointment of Nodal Officers***: Every public entity is mandated to appoint a nodal officer within 30 days of the RoW Rules' commencement. The nodal officer's role includes overseeing right-of-way processes and facilitating communication between public entities and telecommunications facility providers.
- ***Applications for Underground and Overground Networks***
  - *Underground Networks*: Facility providers seeking to establish underground networks must submit applications via the designated portal, with public entities required to approve or reject applications within 45 days. A failure to act within this timeframe results in automatic approval.
  - *Overground Networks*: Providers applying for overground networks must do so through the portal, with provisions allowing for the use of public street furniture to install telecommunications equipment. Public entities have a 45-day window to approve or reject applications, after which permissions are deemed granted.
- ***Temporary Overground Networks***: In scenarios where damage occurs to existing networks, facility providers are permitted to establish temporary overground networks without prior permission. However, the restoration of original infrastructure must be completed within a stipulated period of 60 to 90 days.
- ***Automatic Permissions for Special Projects***: The Central Government may designate specific projects as "special telecommunications projects," wherein right of way permissions are automatically granted upon application.
- ***Rights and Obligations of Property Owners***: Property owners can request the removal, relocation, or alteration of telecommunications infrastructure with 30 days' notice. Additionally, any actions planned by property owners that could interfere with telecommunications infrastructure must be reported to facility providers through the designated portal.
- ***Damages and Compensation***: In instances where property owners' actions result in damage to telecommunications infrastructure, they are required to compensate the facility provider for the cost of repairs. Any related disputes will be addressed under the Telecom Act.

The RoW Rules mark a pivotal step toward modernizing India's telecommunications framework by simplifying the right of way processes. These streamlined and clear regulations will facilitate faster rollout and expansion of telecommunications services while ensuring safety, fairness, and collaboration between public entities, private property owners, and telecommunications service providers. The RoW Rules promise not only enhanced network deployment efficiency but also support India's broader goal of advancing digital connectivity, fostering economic growth, and driving technological innovation.

---

6. Other Telecommunications Updates

- **TRAI releases Consultation Paper on Review of the TCCCPR, 2018, due to** a range of issues observed during the implementation of TCCCPR 2018, such as misuse of registered headers and content templates, as well as insufficient complaint redressal mechanisms. Key pointers raised in the Consultation Paper include refining the definitions of commercial communications to address ambiguities such as simplifying meaning of transactional, service (explicit and inferred), and promotional messages; enhanced mechanisms to improve the effectiveness of the current complaint redressal process such as real-time transfer of complaints and immediate action on suspected UCC; introduction of more stringent financial penalties and stricter measures against senders and telemarketers who violate UCC rules; introduction of better traceability mechanisms to detect and act against UCC violations, etc.

- **DoT released the draft Telecommunications (Adjudication and Appeal) Rules under the Telecom Act for public consultation**, outlining procedures for resolving telecom-related disputes, particularly breaches of telecom licenses, radio frequency assignments, and other contraventions specified in the Act.

- **TRAI issues recommendations on framework for service authorizations under the Telecom Act, on** September 18, 2024, following the provision under Section 3(1)(a) of the Telecom Act, which stipulates that any entity intending to provide telecommunication services must obtain authorization, subject to specified terms, conditions, fees, and charges. The DoT had sought TRAI's recommendations regarding the structure and requirements for such authorizations. TRAI's key recommendations to the Government discuss among other aspects, service

authorizations frameworks under Section 3(1) of the Telecom Act rather than entering into agreements with entities; regulation of encryption equipment; safeguarding confidentiality and privacy and ensuring that authorised entities' telecommunication network infrastructure and equipment are located within India along with other data localization requirements.

- **DoT notified the Digital Bharat Nidhi Rules, 2024 ("DBN Rules"), as the first set of rules under the Telecom Act,** replacing the Universal Service Obligation Fund ("**USOF**"). The DBN Rules aim to fund telecom services in underserved areas through a Universal Access Levy ("**UAL**"), set at 5% of the telecom company's adjusted gross revenue. While the DBN Rules come into effect immediately, they don't override existing arrangements until they expire.

  .

- **TRAI issued directions titled "The Standards of Quality of Service of Access (Wireline and Wireless) and Broadband (Wireline and Wireless) Service Regulations, 2024",** on August 2, 2024, for unifying the QoS standards for access (fixed and mobile) and broadband services, superseding three earlier regulations that separately covered basic telephone, cellular mobile, and broadband services. This update comes as the telecom landscape has evolved significantly, particularly with the rise of 4G, 5G, and high-speed fibre-based broadband.

- **TRAI releases Consultation Paper on spectrum assignment for satellite-based commercial communication services,** on September 27, 2024, focusing on the terms and conditions for assigning spectrum to satellite-based commercial communication services. The Consultation Paper aims to address key regulatory and operational aspects to enhance India's satellite communication sector, covering both Non-Geostationary Satellite Orbit **("NGSO")** and Geostationary Satellite Orbit **("GSO")** based services and discusses issues related to assignment of spectrum, spectrum charging mechanism, spectrum assignment conditions, etc.

EMERGING TECHNOLOGY

1. MIB Advisory on Foreign Satellite Usage for Broadcasters

The MIB has issued a **new advisory** dated July 10, 2024, mandating all broadcasters to obtain approval from the Indian National Space Promotion and Authorization Center ("**IN-SPACe**") before utilizing foreign satellite capacity. This directive aligns with the IN-SPACe Norms, Guidelines, and Procedures under the Indian Space Policy 2023, particularly focusing on the authorization of GSO and NGSO satellites.

The advisory specifies that while current lease agreements involving non-indian satellites may continue until March 31, 2025, any new contracts or additional capacity involving such satellites will require explicit authorization from IN-SPACe. Post-March 2025, only IN-SPACe authorized non-Indian satellites will be permitted to provision capacity for communication and broadcast services in India.

Luthra and Luthra
LAW OFFICES INDIA

KEY CONTACTS

Avisha Gupta
Partner
Email - avishag@luthra.com

Somya Yadav
Associate
Email - syadav@luthra.com

Eishani Patnaik
Associate
Email - epatnaik@luthra.com

OFFICES

NEW DELHI
1st and 9th Floors, Ashoka Estate,
24 Barakhamba Road, New Delhi - 110 001
T: +91 11 4121 5100 F: +91 11 2372 3909
E: delhi@luthra.com

BENGALURU
3rd Floor, Onyx Centre, No. 5, Museum Road,
Bengaluru - 560 001
T: +91 80 4112 2800 / +91 80 4165 9245
F: +91 80 4112 2332
E: bengaluru@luthra.com

CHENNAI
Prestige Palladium Bayan,
8th Floor, Greams Road, Nungambakkam Division,
Egmore, Chennai - 600 006,
Tamil Nadu
T: +91 95604 88155
E: chennai@luthra.com

MUMBAI
20th Floor, Indiabulls Finance Center,
Tower 2 Unit A2, Elphinstone Road,
Senapati Bapat Marg, Mumbai - 400 013
T: +91 22 4354 7000 / +91 22 6630 3600,
F: +91 22 6630 3700
E: mumbai@luthra.com

HYDERABAD
Regus Midtown, Office No.131
Level 1, Midtown Building
Road No.1, Banjara Hills,
Opp. Jalgam Vengal Rao Park
Hyderabad, Telangana - 500034
T: +91 40 7969 6162
E: hyderabad@luthra.com