Luthra and Luthra
LAW OFFICES INDIA

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

APRIL – JUNE, 2024

INSIDE

And many more....

In the **April-June 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 framework for Self-Regulatory organizations in the fintech sector

The RBI vide circular dated May 30, 2024, issued a **framework** **("Framework")** for Self-Regulatory Organisations in the fintech sector **("SRO-FT"),** signalling a proactive step towards balancing innovation with regulatory prudence. Earlier, a draft version of this Framework was released on January 15, 2024, by RBI for public comments.

The Framework inter alia outlines the key characteristics and functions, governance standards, eligibility criteria and expectations for grant of recognition as an SRO-FT, briefly summarized below.

- ***Eligibility and Membership requirements:*** It includes general requirements such as registration as a not-for-profit company per Section 8 of the Companies Act, 2013, minimum net-worth criteria, membership requirements from representatives of fintech sector, 'fit and proper' criteria of Board of Directors and Key Managerial Personnel, application requirements for SRO-FT and the right of RBI to have final decision in regards to the grant of recognition to any SRO-FT. Membership in the SRO-FT should be primarily from fintechs that are currently not regulated by any financial sector regulator. Membership may also be open to regulated entities (other than banks).
- ***Governance and Management:*** SRO-FT should be professionally managed with its Articles of Association ("**AoA**") containing appropriate provisions to ensure the same. The AoA should contain criteria for admission, suspension, expulsion and re-admission of its members. Further, there should be a structure put in place by the Board of the SRO-FT to monitor the 'fit and proper' status of its directors. Additionally, provision has been made for the RBI to nominate/depute Observer(s) on the Board of the SRO-FT, if it deems necessary.
- ***Establishing technology standards:*** SRO-FTs are expected to set baseline technology standards for its members so as to leverage technology-driven solutions for monitoring and reporting.
- ***Duties towards RBI:*** SRO-FTs will be entrusted with responsibilities such as developing industry-wide codes of conduct, conducting self-assessments, and recommending regulatory enhancements to the RBI. They must also set baseline governance standards for their members (for transparency, disclosure, data privacy), regularly update RBI on developments in the sector to aid in policy

making and notify any major violation by its members for RBI to initiate timely action. SRO-FTs must also submit annual report and periodic returns, as may be prescribed, to the RBI.

- ***Oversight mechanisms*:** SRO-FTs must establish appropriate surveillance mechanisms for effective monitoring and must specify the penalties for violation of agreed rules/ codes of conduct deployed.
- ***Autonomy*:** The SRO-FT should function independently devoid of any influence from any single member or group of members.
- ***Grievance redressal:*** SRO-FTs must establish a fair and transparent procedure for dispute redressal and resolution of grievances arising amongst members.

By empowering SRO-FTs, the RBI aims to create a collaborative ecosystem where industry stakeholders play a pivotal role in setting and enforcing standards, codes of conduct, and best practices. This approach not only streamlines regulatory compliance but also encourages innovation by providing a structured platform for dialogue between regulators, fintech firms, and other market participants. This collaborative governance model thereby enhances regulatory agility along with fostering a conducive environment for sustainable fintech growth.

Several associations currently include fintech firms as members, functioning as self-regulatory bodies within the industry. It is anticipated that these associations will seek SRO-FT recognition. However, they primarily represent fintechs focused on specific activities such as digital lending. To gain RBI approval as an SRO-FT, these associations may need to expand their membership to include fintech players from other sectors. It should be noted that the regulatory framework allows for multiple organizations to be considered for SRO-FT status, encouraging fintech firms to join at least one SRO. It remains to be seen how multiple SROs, if permitted, will coexist and whether they can establish different standards or codes of conduct for the same fintech activities.

2. RBI issues draft directions on the Regulation of Payment Aggregators ("PAs") – physical point of sale

With the aim to enhance the transparency, security, and reliability of payment services in India, the RBI on April 16, 2024 released draft **directions** **("Draft Directions")** broadening the ambit of its PA regulations to include physical point-of-sale **("P-POS")** payment providers. P-POS will now be required to apply for authorization from the RBI and must adhere to a series of detailed guidelines related to merchant onboarding,

customer grievance redressal, and other key operational standards as outlined under the 'Guidelines on Regulation of Payment Aggregators and Payment Gateways' issued by the RBI on March 17, 2020 **("2020 PA-PG Guidelines").**

Some of the key requirements outlined under the Draft Directions are envisaged below:

- ***Authorization:*** Non-banking entities providing P-POS services must inform the RBI about their intentions to seek PA authorization within 60 calendar days from April 16, 2024 regarding their existing P-POS activities. Further, these P-POS providers have been given a deadline of May 31, 2025, to apply for a PA license. Additionally, non-banking P-POS providers must seek approval from the Department of Payment and Settlement Systems (DPSS), RBI and the Central Office (CO) in the same manner.
- ***Minimum net worth*:** Existing non-banking P-POS providers are required to have a net worth of at least ₹15 crore when submitting their application for authorization. Furthermore, existing P-POS providers are required to achieve a net worth of at least ₹25 crore by March 31, 2028.
- ***Merchant Onboarding*:** Non-banking P-POS providers must conduct thorough due diligence to verify the legitimacy and financial stability of the merchants. The onboarding process must ensure that only credible and reliable merchants are allowed to use P-POS services, thereby safeguarding the payment ecosystem.
- ***Customer Grievance Redressal*:** P-POS providers must establish a robust customer grievance redressal mechanism by setting up dedicated helplines and support teams to address customer complaints and queries promptly. Providers must ensure that all grievances are resolved within a stipulated timeframe, and customers are kept informed about the status of their complaints.
- ***Compliance with Data Security Standards*:** P-POS providers must implement security measures such as encryption of data, regular security audits, and compliance with industry standards such as Payment Card Industry Data Security Standard (PCI DSS), to protect sensitive customer data from breaches and cyber-attacks. P-POS providers must also establish protocols for data breach response and notification to minimize the impact of any security incidents.

- ***Regulatory Reporting*:** P-POS providers are required to submit regular reports to the RBI detailing their operational activities, financial performance, and compliance status.

It is to be noted that the applicability of the 2020 PA-PG Guidelines did not extend to offline PAs operating in physical spaces via POS machines which created different regulatory standards for offline and online PAs. The inclusion of P-POS providers within the scope of RBI's PA regulations would bring these providers under regulatory oversight. This move is likely to boost consumer confidence in digital payment solutions and encourage wider adoption of P-POS services across various sectors.

For P-POS providers, the Draft Directions presents both challenges and opportunities. While the operational and compliance requirements may necessitate significant investments in systems, processes, and personnel, they also offer an opportunity to build stronger, secure and more customer-centric operations. Further, P-POS providers that successfully meet the regulatory standards are likely to gain a competitive advantage in the market, as they can assure merchants and customers of their credibility and reliability. Moreover, the emphasis on financial stability through stringent net worth requirements ensures that only well-capitalized entities operate in the P-POS space. This reduces the risk of financial instability and potential failures, which could disrupt the payment ecosystem and harm consumer trust.

The Draft Directions ensure that all existing non-banking P-POS providers are brought under the regulatory umbrella within a specified timeframe, thereby enhancing the overall integrity and reliability of the payment ecosystem. As the regulatory landscape evolves, this move is expected to foster greater consumer confidence, drive wider adoption of digital payments and support the growth of India's digital economy.

3. RBI issues clarifications in respect of PAs – Online and P-POS

In furtherance to the aforementioned Draft Directions, the RBI vide **press release** dated April 16, 2024 provided for clarifications in respect of PAs – Online and P-POS **("Clarifications")** updating inter alia, the Know your Customer **("KYC")** and due diligence requirements of merchants, operations in escrow accounts and similar compliance requirements under the 2020 PA-PG Guidelines. The Clarifications shall be applicable with effect from one month from its date of issue (unless otherwise specified) to all PAs, irrespective of status of the application submitted to the RBI for seeking authorisation.

The key modifications/ clarifications in respect of PAs – Online and P-POS include:

- ***Escrow account:*** Funds related to Delivery versus Payment (DvP) transactions, previously not covered under the scope of the existing RBI circulars must be routed through the escrow account(s) opened by the PA. Cash-on-delivery transactions to fall outside the scope of the RBI circulars on PA, hence, to not be routed through escrow accounts. Further, the provision permitting debit to escrow accounts for "payment to any other account on specific directions from the merchant," under the 2020 PA-PG Guidelines, has been deleted with immediate effect.
- ***KYC and Due Diligence****:* PAs must now perform due diligence of merchants they onboard in accordance with the Customer Due Diligence **("CDD")** requirements outlined in the Master Directions on KYC **("MD-KYC"),** 2016, as amended on January 4, 2024. Further, PAs must comply with the wire transfer guidelines as per MD-KYC 2016, as amended. These instructions are to be applicable three months from April 16, 2024.
- ***Merchant Due Diligence***: Categorisation of merchants into small and medium merchants and varied degree of due diligence requirements to be undertaken.
    - **Small Merchants**: PAs must conduct Contact Point Verification **("CPV")** of the business establishment and verify the bank account where funds are settled.
    - **Medium Merchants**: PAs must perform CPV and verify one Officially Valid Document **("OVD")** of the proprietor or beneficial owner and one OVD of the business.
    - **Video-based Customer Identification Process ("V-CIP"):** Assisted V-CIP is allowed with the help of an agent at the merchant end. PAs must maintain records of the agent assisting the merchant.
- ***Ongoing Merchant monitoring:*** PAs must monitor merchant transactions continuously and migrate merchants to higher CDD categories based on transaction patterns. Additional due diligence should be performed immediately upon migration. PA's need to consistently check that transactions processed by PAs must align with the merchant's business profile. Further, risk-based payment limits to be established for onboarded merchants.
- ***Timeline for due-diligence completion*:** Existing PAs, both authorised and those with pending applications, must complete the due diligence process for all existing merchants by September 30, 2025. Entities offering P-POS services

must complete this process within 12 months from their application submission date. Quarterly compliance reports must be submitted to the RBI's regional office.

- ***Storage of Card-on-File ("CoF") data***: From August 1, 2025, entities in the card transaction/payment chain other than card issuers and networks will not be allowed to store CoF data. Previously stored data must also be purged by such entities. For transaction tracking or reconciliation, limited data (last four digits of the card number and the card issuer's name) can be stored in compliance with applicable standards.

These steps will significantly reduce security and privacy risks arising from storage of card data and possibility of data leaks. Notably, the requirement for marketplaces to open escrow accounts and settle funds might increase friction and cost for the marketplaces since earlier these marketplaces used to majorly settle funds directly to sellers via a PA. Further, the KYC norms lack clarity on the terms "due diligence" and "CPV" which have not been adequately defined. This ambiguity might construe different interpretations of these terms which pose a risk to uniformity in understanding of the KYC obligations for applicable stakeholders. It remains to be seen how these updated directions unfold amongst the fintech industry and its concerned stakeholders.

---

4. Other Fintech Updates

- **RBI has released new draft guidelines on a comprehensive regulatory framework for aggregation of loan products by lending service providers ("LSPs"), in April, 2024,** which interalia includes extensive guidance to LSPs to ensure transparency in loan offers; unbiased presentation of loan options via non-usage of 'dark patterns'; displaying essential loan information; etc. These guidelines bring loan aggregators under the RBI's regulatory ambit to curb mis-selling practices and ensure a fair and transparent lending experience for borrowers in India.
- **RBI has proposed draft master directions for electronic trading platforms("ETPs") in May 2024**, establishing a comprehensive revised regulatory framework for ETPs which interalia includes obligations on stringent eligibility criteria for ETP operators, robust governance frameworks to ensure operational integrity, and mechanisms for risk management and surveillance.

IT AND DATA PROTECTION

1. IT Ministry introduces mandatory security requirements for Closed-Circuit television ("CCTV") cameras

On April 9, 2024, the Ministry of Electronics and Information Technology **("MeitY")** vide **gazette notification** amended the Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021 **("2021 Order")** to include mandatory security parameters for CCTV cameras.

The key security requirements under the 2021 Order are delineated as follows:

- ***Physical Security*:** CCTV cameras must utilize tamper-resistant enclosures and locking mechanisms to prevent physical tampering.
- ***Access Control*:** Robust access control systems with authentication, role-based access control (RBAC), and regular reviews of access permissions are mandatory. This ensures only authorized personnel can access footage.
- ***Network Security*:** Data transmission must be encrypted to safeguard sensitive information captured by CCTV systems.
- ***Software Security:*** Regular software updates, disabling unused features, and enforcing strong password policies are crucial to minimize vulnerabilities.
- ***Penetration Testing*:** Regular penetration testing helps identify and address weaknesses in the CCTV system's defences against cyberattacks.

Regards implementation, these new requirements will come into effect six months after the notification date. The 2021 Order further prohibits the manufacture, sale, or distribution of non-compliant CCTV systems. Manufacturers must obtain registration from the Bureau of Indian Standards **("BIS")** after product testing by BIS-recognized labs.

This development is particularly important given the increasing use of CCTV systems in public spaces, often capturing sensitive biometric data. Earlier this year, the Indian Railways faced criticism for its plan to install face-detection CCTV cameras in coaches. Similarly, the Lucknow police proposed using facial recognition technology for crowd management during elections, raising privacy concerns. These new requirements vide the 2021 Order demonstrate the Government's commitment to balancing security needs with data privacy. By mandating enhanced security measures for CCTV systems,

the Government aims to mitigate cyberattacks and protect sensitive information collected in public spaces.

2. SEBI issues guidelines to prevent sharing of real-time stock exchange data with online gaming platforms

On May 24, 2024, the Securities and Exchange Board of India **("SEBI")** issued a **circular** envisaging norms aimed at controlling the dissemination of real-time share prices or price data **("price data")** to third parties such as online gaming platforms involved in virtual trading and fantasy games **("Circular")**. These norms have been notified to tackle the issue of misuse or unauthorised use of data via subsequent sharing of market price data to and by online gaming platforms, apps, websites, etc., who provide virtual trading services or fantasy games based on real-time movement of price data of listed companies. This move comes in response to concerns raised by SEBI's Secondary Market Advisory Committee (SMAC) regarding the potential misuse and unauthorized use of such critical financial data.

According to the Circular, SEBI has mandated the following:

- ***Applicability***: The norms will be applicable to i) recognised stock exchanges, ii) recognised clearing corporations, iii) depositories, and iv) registered market intermediaries.
- ***Enforcement Date:*** The provisions of the Circular shall be applicable from the 30th day of issuance of the Circular i.e., from June 24, 2024.
- ***Restriction on unauthorised use of data*:** The Stock Exchange, Clearing Corporation and Depositories (collectively referred to as Market Infrastructure Institutions ("**MIIs**")) and registered market intermediaries have to ensure that no price data is shared with any third party except in situations where such sharing is required for orderly functioning of the securities market or for fulfilling regulatory requirements.
- ***Data sharing arrangements***: MIIs or market intermediaries are required to enter into appropriate agreements with entities, with whom they intend to share price data. Such agreement must lay down the specific activities for which such price data will be used. It should also include justification as to why such price data is required for orderly functioning of securities market. The list of entities and activities for which price data is being shared shall be reviewed at least once in a financial year by the MIIs or market intermediaries.

- ***Education and awareness activities:*** Price data may be shared for investor education and awareness activities without offering any kind of monetary incentive to participants, with a lag of one day.
- ***Due diligence***: MIIs and market intermediaries are required to exercise appropriate due diligence while sharing price data.

Previously, the National Stock Exchange of India **("NSE")** had issued warnings against the use of real-time market data for online gaming activities in April 2023. The NSE had emphasized that sharing such data for gaming purposes contradicts the principles of fair and transparent trading. In a circular addressed to all trading members, the NSE reiterated that its market data is exclusively meant for legitimate trading activities by clients and should not be used for gaming or virtual trading purposes. This regulatory stance reflects longstanding apprehensions among exchanges and regulators regarding online trading games. As early as 2016, SEBI had cautioned investors about the risks associated with online stock games offered by the Bombay Stock Exchange **("BSE")** and the NSE. These games allowed participants to speculate on stocks, currencies, and commodities, posing potential risks and liabilities for unsuspecting investors. The BSE explicitly warned investors that participating in such schemes was at their own risk and that these activities were neither approved nor endorsed by the exchange.

We note that this move by SEBI aims to hold accountable those entities that have access to market data, placing the responsibility on them to ensure compliance with the Circular. By imposing stringent guidelines and enhancing oversight mechanisms, SEBI aims to reinforce transparency, fairness, and investor protection within the financial ecosystem. The ongoing efforts to align market practices with regulatory expectations highlight the evolving challenges in regulating the intersection of digital platforms and financial markets.

---

3. Other IT and Data Protection Updates

- **SEBI has approved norms to regulate unregistered financial influencers and has notified a Cybersecurity and Cyber Resilience Framework for SEBI regulated entities vide press release dated June 27, 2024**, which outlines the proposals approved by the SEBI in its 206th board meeting. These norms interalia provide for directions to restrict associations of SEBI regulated entities with

unregistered individuals providing advice, recommendation and claim of return or performance related to securities.

- **Ministry of Labour and Employment has mandated deployment of Facial Authentication Technology by the Employee's Provident Fund Organisation for Employee Pension Scheme pensioners to ease the Digital Life Certificate ("DLC") submission on June 08,2024**, which interalia provides for pensioners to use the Unique Identification Authority of India **("UIDAI")** Facial Recognition App on any android based smartphone for the submission of DLCs, thereby easing accessibility.

E-COMMERCE

1. Supreme Court issues directives to address misleading advertising practices.

Vide **order** dated May 7, 2024, the Supreme Court **("SC")** in the case of *Indian Medical Association & Anr.* ***("IMA")*** *v. Union of India,* 2024 SCC OnLine SC 931, has emphasized that the fundamental right to health encompasses the consumer's right to be informed about the quality of products offered by manufacturers, service providers, advertisers, and advertising agencies. In this order, the SC highlighted the absence of a robust legal mechanism which ensures compliance with the Guidelines for Prevention of Misleading Advertisements and Endorsements of Misleading Advertisements, 2022 **("2022 Guidelines").**

This order addressed critical issues pertaining to misleading advertisements, specifically focusing on accusations against Patanjali Ayurved for disseminating misleading information and casting aspersions on allopathic medicine. The petition, filed by the IMA highlighted concerns regarding false claims made by Patanjali in its advertisements despite assurances given to the SC regarding their withdrawal.

Expanding its scrutiny to encompass misleading advertisements in general, the SC issued directives aimed at various stakeholders, including advertisers, endorsers, and regulatory bodies. Observing the pervasive impact of endorsements by celebrities, influencers, and public figures, the SC emphasized their accountability in endorsing products without fully understanding potential consequences. It underscored the necessity for endorsers to possess adequate knowledge or experience of the products they endorse to ensure transparency and prevent deception. This directive was part of a broader initiative to enforce stricter compliance with existing regulations governing advertisements.

To address the regulatory vacuum, the SC, interalia, issued directives that mandated several key actions, which are mentioned below:

- ***Self-declaration by Advertisers and Agencies*:** Before any advertisement is printed, aired, or displayed for TV/Radio advertisements, advertisers or advertising agencies must submit a self-declaration aligning with Rule 7 of the Cable Television Networks Rules, 1994, and such declaration must be uploaded on the Broadcast Sewa Portal under the Ministry of Information and Broadcasting **("MIB").** For advertisements in print media or on the internet, the

MIB was directed to establish a dedicated portal within four weeks to facilitate similar self-declarations.

- ***Responsibility of Endorsers*:** Celebrities, influencers, and public figures endorsing products were cautioned about their responsibility in ensuring the accuracy and fairness of their endorsements. The SC stressed that such endorsements should reflect genuine opinions based on adequate information or experience with the endorsed products.
- ***Action by Consumer Protection Authorities*:** The Ministry of Consumer Affairs, Food, and Public Distribution and the Ministry of Health and Family Welfare were instructed to provide detailed reports on actions taken by regulatory bodies like the Central Consumer Protection Authority **("CCPA")** and the Food Safety and Standards Authority of India (FSSAI).
- ***Penalties and Enforcement*:** Under the Consumer Protection Act, 2019, the CCPA was empowered to impose penalties up to INR 10 lakh for the first instance of misleading advertisements by manufacturers, advertisers, or endorsers. Subsequent violations could attract higher penalties up to INR 50 lakh, with provisions for banning endorsers from participating in endorsements for specified periods upon repeated offenses.

These directives were pronounced as binding law under Article 141 of the Constitution of India. The SC underscored the shared responsibility of advertisers, advertising agencies, and endorsers in preventing false and misleading advertisements. It further directed advertisements to not be disseminated on relevant channels or media platforms without first uploading the mandated self-declaration as afore mentioned. Additionally, the bench expressed concern over the lack of detailed information on the nature of actions taken by the authorities, which also has the power to initiate action suo moto. It directed the Ministry of Consumer Affairs to submit an additional affidavit detailing actions against misleading advertisements, especially in the food and health sectors. The SC also highlighted discrepancies in enforcing the Advertisement Code, noting only 60 instances of action against broadcasters since 2018.

Following the SC's directives, MIB has mandated a self-declaration certificate for all new advertisements from June 18, 2024. In this mandatory declaration, advertisers have to certify that the ads, in question, do not contain "misleading claims" and comply with all relevant regulatory guidelines including those stipulated in Rule 7 of the Cable Television Networks Rules, 1994 and the Norms of Journalistic Conduct of Press

Council of India. Ongoing advertisements, however, do not require self-certification currently.

We note that vide circular issued on July 3, 2024, the MIB has issued an advisory to concerned advertisers, advertising agencies and media stakeholders, pursuant to the Supreme court order dated May 7, 2024, clarifying that the requirement for uploading self-declaration certificates on the Broadcast seva portal for TV/radio advertisements and on the Press Council of India portal for advertisements on print media/internet has to now be done annually and shall extend only to advertisers/advertising agencies issuing advertisements for products and services related to food and health sectors. Further, only these advertisers are required to make available the proof of uploading the self-declaration to the concerned media stakeholders such as TV channels, newspapers, entities involved in publishing of advertisements on the internet, etc.

The SC has scheduled this matter for further hearing on July 9, 2024, stressing the ongoing importance of addressing misleading advertising practices to safeguard consumer rights and uphold legal standards. In conclusion, these SC directives mark a significant step towards strengthening consumer protection laws in India. By emphasizing transparency, accountability, and compliance with regulatory norms, the SC's rulings seek to create a more equitable and trustworthy marketplace for consumers. Moving forward, these directives are expected to set a precedent for ethical advertising practices and responsible endorsements, thereby promoting consumer welfare and upholding the integrity of the advertising industry in India.

---

2. Other E-Commerce Updates

- **Department of Consumer Affairs ("DoCA") has released draft Guidelines ("DoCA Guidelines") for the Prevention and Regulation of Unsolicited and Unwarranted Business Communication, 2024 on June 20, 2024**, addressing communication for sale or promotion of goods and services that is neither as per the consent nor as per the registered preferences of the recipient. The DoCA Guidelines interalia outline specific conditions that classify a communication as unsolicited, such as using unauthorized number series or SMS headers, contacting recipients who have opted out, failing to obtain digital consent, etc.

TELECOMMUNICATION

1. The Department of Telecommunications ("DoT") has issued additional instructions for KYC verification of business users

The DoT **vide** notification dated May 20, 2024, has issued additional instructions regarding the KYC verification of business users **("Instructions").** The key highlights of the Instructions are as follows:

- In cases where ***end users are not identifiable in a business connection*** such as SIMs obtained for research and development & testing activities for a specified purpose etc., the requirement of end user KYC is optional. However, for this category of customers, mobile connections shall be issued by the licensee's employees only.
- Before issuing such connections, the licensee shall ***obtain an undertaking*** from the subscribing entity detailing the use case scenarios having no end users of the business connections and the licensee shall reasonably satisfy itself that the undertaking from the subscribing entity detailing the use case scenarios is realistic.
- In cases of ***physical verification of the entity's address and premises*** before issuing such connections, the Licensee shall verify that the proposed use case scenarios of the subscribing entity are realistic. Further, the Licensee shall also monitor the bonafide use of such connections by the subscribing entities.
- The licensees shall provide such connections with ***limited call/SMS/data facility with definite validity period of maximum one year at a time*** as per the use case scenarios of subscribing entity. During the renewal of validity for such connections, the licensee shall satisfy itself by usage patterns from the past as well as proposed usage for the upcoming year.
- Licensee shall ***limit the issuance of such connections*** to a maximum number upto 100 for any given entity at a given time.
- Such connections shall ***not be used for Machine to Machine ("M2M") communication services***.
- The ***list of such connections along with the details of restrictions*** shall be provided separately to LSAs on monthly basis for audit and also to LEAs as and when sought.

Notably, the earlier KYC directions were introduced in August 2023 as an attempt to curb cyber fraud. Under such directions the DoT discontinued the "bulk connection" category and replaced it with "business connections". Among other things, to issue business connections, telecom companies were required to obtain information such as business corporate Identity Number (CIN)/business license/trade registration, Goods and Services Tax (GST) certificate (if applicable). Further, the businesses were also required to provide telecom companies with a list of end-users who would be using those business connections. Furthermore, in cases of change in end users, the businesses were required to inform their telecom company about the change and the new end-user was mandatorily required to re-verify the connection under their name within 7 days. The telecom companies faced practical challenges in implementing the earlier KYC directions owing to the reason that in certain cases, the identity of the end users could not be traced. Hence, the issuance of the Instructions issued by the DoT is a step in the right direction as it would provide guidance in cases where end users are not identifiable.

2. Telecom Regulatory Authority of India ("TRAI") has released consultation paper on National Broadcasting Policy 2024

The TRAI **vide** circular dated April 02, 2024, released a consultation paper titled 'Inputs for Formulation of National Broadcasting Policy-2024' **("NBP").** This initiative follows a request from the MIB in July of the previous year, asking TRAI for input on formulating the policy. In response, TRAI issued a pre-consultation paper in September, seeking comments on the issues to be included. Post which the TRAI published the consultation paper on NBP.

The consultation paper on NBP aims to enable formulation of a national policy and intends to target a broad roadmap for next 10 years with special focus on next 5 years. Further, it delves into the existing issues of the sector, highlighting their trends and projections, initiatives taken by the Government, exploring the international best practices and aims to come out with inputs for policy formulation with focussed strategies and achievable targets to position India's broadcasting sector at the global stage.

The issues for consultation for the NBP are as follows:

- Vision, mission, preamble, and objectives of the NBP.
- Parameters for measuring the broadcasting sector's revenue, employment generation, subscription figures, etc.

- Strategies for the government to provide affordable TV services, augment research and development capabilities, promote indigenous manufacturing, generate employment, support startups, and develop skills.
- Policies to turn India into a global content hub and promote local talent and creators.
- Measures to promote India as an uplinking hub.
- Strategies to strengthen public service broadcasting and promote quality content creation and dissemination.
- Policies to promote Indian content on Over-the-top (OTT) platforms.
- Regulatory measures for promoting online gaming while ensuring public protection.
- Broadcasting sector's role in fulfilling social and environmental responsibilities, empowering various communities, and utilizing technology for disaster alerts.

The broadcasting sector is a sunrise sector having huge potential to contribute towards the growth of the Indian economy. The inputs for formulation of policy aim at stipulating the vision, mission, objectives and strategies for the planned development and growth of the broadcasting sector in the country in the era of new and emerging technologies. The consultation paper on NBP issued by TRAI is a comprehensive effort to address the multifaceted challenges and opportunities in India's broadcasting sector, aiming to foster growth, innovation, and social responsibility.

3. Central Government partially implements Telecommunications Act, 2023 ("New Telecom Act") from June 26, 2024.

On 21 June, 2024, the Central Government vide **gazette notification** issued order for partially enforcing certain provisions under the New Telecom Act starting June 26, 2024. The New Telecom Act is set to supersede the Indian Telegraph Act of 1885, the Wireless Telegraphy Act of 1933, and the Telegraph Wires (Unlawful Possession) Act of 1950.

The sections which have been implemented include Sections 1, 2, 10 to 30, 42 to 44, 46, 47, 50 to 58, 61 and 62 of the New Telecom Act which enforce the clauses on Definitions, Right of Way framework, common ducts, telecom standards, national security and public safety, technology development, user protection, etc., among others.

The key sections which have been enforced have been briefly delineated below:

- ***Government Control and National Security***: The Government has the authority to take over the control and management of any or all telecommunication services or networks in the interest of national security, maintaining friendly relations with foreign states, or during wartime.
- ***Interception of messages and suspension of services:*** The Central Government has the authority to order interception of messages and suspension of services in event of a public emergency or in interest of public safety. The provision further allows the Government to stop the transmission of any message or class of messages "relating to any particular subject". However, disclosure of messages must be "in intelligible format".
- ***Transformation of USOF:*** Provision of rebranding of the Universal Service Obligation Fund **("USOF")** as the Digital Bharat Nidhi which not only symbolizes a shift in focus but also broadens the scope of the USOF. Previously, USOF was primarily used to support the establishment of telecommunication services in rural and remote areas. However, under the New Telecom Act, the Digital Bharat Nidhi will also be available for funding research and development projects and pilot initiatives.
- ***User Protection Against Spam and Malicious Communications:*** Provisions aimed at protecting users from spam and malicious communications. This is a critical addition, given the growing prevalence of spam calls, messages, and other forms of Unsolicited Commercial Communication **("UCC")**.
- ***Non-Discriminatory and Non-Exclusive Rights of Way:*** Enforcement of non-discriminatory and non-exclusive rights of way for telecom network rollouts.
- ***Establishment of Common Ducts and Cable Corridors:*** The Central Government has the power to establish common ducts and cable corridors.
- ***Creation of Regulatory Sandboxes:*** The Government will be able to create regulatory sandboxes where new products, services, processes and business models can be tested on a limited set of users without having to comply with all the obligations underlined under the New Telecom Act.
- ***Suspension/removal of telecom equipment/services:*** The Central Government is empowered to order suspension, removal or prohibition of specified telecom equipment and services from notified countries or persons for national security reasons.

We note that the sections enforced under the New Telecom Act majorly provide for positive measures that are critical in ensuring that the telecommunication infrastructure remains secure and resilient, particularly in times of crisis. The ability to assume control over telecommunication networks provides the Government with the flexibility to

respond swiftly to threats and emergencies. This is particularly important given the increasing reliance on digital communication and the potential vulnerabilities that come with it. By implementing stringent measures to curb spam and malicious communications, the New Telecom Act seeks to enhance consumer experience and trust in telecommunication services. These measures are expected to include stricter penalties for offenders, improved reporting mechanisms, and enhanced collaboration between service providers and regulatory authorities to tackle the issue effectively.

Further, the expanded mandate on Digital Bharat Nidhi is expected to spur innovation in the telecommunication sector, encouraging the development of new technologies and services. By investing in research and development, India can stay at the forefront of technological advancements and ensure that its telecommunication infrastructure is capable of meeting future demands. Non-discriminatory and non-exclusive grants of right of way for telecom network roll-out can also streamline the process of infrastructure development, ensuring that all service providers have equal opportunities to deploy their networks. By removing barriers and creating a level playing field, this move encourages competition and innovation in the telecommunication sector which can lead to better services and more choices for consumers. Additionally, this provision is expected to expedite the rollout of advanced telecommunication networks, including 5G, which is crucial for India's digital transformation.

As India continues its digital transformation journey, the New Telecom Act is expected to play a pivotal role in shaping the future of the telecommunication sector, however, certain segments of industry stakeholders are concerned regarding the potential threat to data privacy and encryption that might arise, by virtue of the power granted to the Government under the New Telecom Act to order for interception of messages on the grounds of public emergency or public safety. Having said that, it remains to be seen how the New Telecom Act addresses these possible concerns.

4. TRAI issues directions to Access Providers under the Telecom Commercial Communication Customer Preference Regulations, 2018 ("TCCCPR 2018")

On June 24, 2024, TRAI issued **directions** **("TRAI Directives")** to Access Providers under the TCCCPR 2018 to aid in regulating UCC. This is part of TRAI's ongoing effort to mitigate the issue of UCC, commonly referred to as spam.

After analysing the existing systems in place for reporting spam and setting customer preferences, the regulatory body identified significant shortcomings such as lack of

direct options/hyperlinks on telecom companies' web portals and mobile apps for registering complaints or setting preferences for commercial communications and manual entry of customer complaint information leading to less ease of accessibility and more inconvenience for consumers in reporting spam.

To address the afore-mentioned inefficiencies, the TRAI Directives primarily envisage the following requirements aimed at telecom companies to enhance the user-friendliness of their mobile apps and web portals:

- Direct options/hyperlinks for registering complaints by consumers and setting preferences for commercial communications should be prominently placed on the companies' main page or home page to ensure ease of access for users.
- Essential complaint details should be automatically populated if the user has granted the telecom company's app permission to access their call logs and other relevant data making it easier for users to lodge valid complaints.

In addition to improving the user interface for reporting spam and setting preferences, TRAI has issued further directives **("TRAI Directives 2")** to enhance the monitoring and enforcement of the TRAI Directives under the TCCCPR 2018.

The expanded reporting requirements under TRAI Directives 2 include:

- Telecom companies to submit performance monitoring reports **("PMRs")** on a monthly basis as opposed to the previous quarterly basis. Further, PMRs to be submitted within ten days from the end of each calendar month starting July 2024.
- PMRs to contain segregation of complaints received about registered telemarketers, unregistered telemarketers, and the communication channels that have been penalized (e.g., blacklisted or disconnected) for repeatedly engaging in unregistered telemarketing activities.
- Telecom companies to provide more detailed information about each complaint, including the nature of the complaint, the actions taken to resolve it, and the outcome.

We note that in order to comply with the new TRAI directives, telecom companies will need to adequately upgrade their systems which may require significant investment in technology and training. Further, these companies will need to implement new processes to gather and report the expanded data required by TRAI. This may involve changes to their internal data collection and reporting systems, as well as increased

coordination among different departments. The stringent reporting requirements and more granular monitoring will increase accountability for telecom companies. They will need to ensure that they are effectively addressing spam complaints and complying with the new TRAI directives to avoid penalties and regulatory action.

While the new directives will require telecom companies to make significant changes, they are ultimately designed to benefit consumers in ways such as easier reporting, reduced spam and greater transparency thereby reducing the overall volume of UCC. The expanded reporting requirements will provide greater transparency into how telecom companies are handling spam complaints and implementing anti-spam measures which will allow consumers to make more informed decisions about their telecom providers.

---

5. Other Telecommunications Updates

- **TRAI has released recommendations on 'Encouraging Innovative Technologies, Services, Use Cases, and Business Models through Regulatory Sandbox in Digital Communication Sector' on April 12, 2024,** which interalia outlines all the relevant components in detail and offer a comprehensive framework for conducting Sandbox testing for the Digital Communication sector.
- **TRAI released recommendations on 'Telecommunications Infrastructure Sharing, Spectrum Sharing, and Spectrum Leasing' on April 24, 2024,** which interalia includes guidance on sharing of passive and active infrastructure, feasibility of issuing instructions to universal service providers (USPs), roaming facilities to other TSPs, possibility of implementing authorized shared access (ASA) technique-based spectrum sharing.
- **TRAI released a consultation paper on "Revision of National Numbering Plan" on June 6, 2024** which interalia delves into issues relating to the allocation of telecommunication identification parameters to all telecommunication devices including devices governing M2M, Internet of Things, 5G related infrastructure and outlines guiding principles such as the need for global best practices for allocation of short codes and discussing a possible chargeable structure for the allocation of telecommunication identifiers.
- **TRAI released recommendations on 'Inputs for formulation of National Broadcasting Policy, 2024' on June 20, 2024**, which interalia outlines

comprehensive proposals and strategies suggested by TRAI such as encouraging proliferation of Indian content; establishing framework enabling growth-oriented policies and regulations through data-driven governance, etc. to assist the DoT in formulating the finalised NBP, 2024.

EMERGING TECHNOLOGY

1. Indian National Space Promotion and Authorization Centre (IN-SPACe) released guidelines, norms, and procedures to implement the Indian Space Policy 2023

On May 3, 2024, IN-SPACe released certain **guidelines** **("IN-SPACe Guidelines")** and important information regarding the space activities which would need authorisation to operate in India. It is stated that only an Indian entity can seek IN-SPACe authorization and any non-Indian entities must do so through an Indian entity, which could be an Indian subsidiary, a joint venture or a collaboration arrangement recognized by the Government of India.

According to the IN-SPACe Guidelines, the general authorization process for space-based services (including satellite communication) interalia includes: (i)submission of the application; (ii) preliminary assessment by IN-SPACe; (iii) providing acknowledgment to the applicant about whether their application is accepted for further processing. The application is analysed on the grounds such as safety and national security, technical radio frequency (RF) interference, compliance with national and international regulatory guidelines, state's liability towards third-party damage from the Indian Space Object, international obligations, geopolitical considerations and relations with foreign countries. Issue of a provisional advisory note by IN-SPACe is needed to enable the applicant to initiate the approval processes with other relevant ministries, issue of authorization/rejection, etc.

The salient features of the IN-SPACe Guidelines interalia delineate the following:

- ***Streamlined process for seeking authorization*** through the IN-SPACe Digital Platform (IDP). A timeline of 75 to 120 days is provided for the approval upon receipt of application of complete application, inter-ministerial/departmental consultations, etc.
- ***Principles for responsible space activities*** such as compliance with all applicable international treaties, Indian laws, and regulations and adherence to globally recognized best practices in cases where there are no specific guidelines.
- ***Applicant's compliance with certain duties*** such as safety and security protocols, mitigating space debris and environmental impacts, procuring mandatory third-party liability insurance, and maintaining transparency.

- ***Eligibility of applicants to seek IN-SPACe authorization for providing communication services over and beyond the Indian territory*** or even exclusively outside the Indian territory. This authorization shall be provided after confirming the validity and regulatory status of the International Telecommunication Union **("ITU")** filing for the intended service area. Communication services over such an area will be subject to regulations of the concerned country's administration.
- ***Criteria for imposition of fine by IN-SPACe to include*** factors such as the nature and gravity of the applicant's actions, their intent and motive, if the actions were caused by reasons beyond their control, penalties already imposed on the applicant by another state authority, and the impact of the applicant's actions on India's national interests including the impact on users. In case the applicant rectifies the discontinuation to the satisfaction of IN-SPACe, IN-SPACe will reserve the right but not an obligation to restore this authorization and/or not to levy the financial penalty.

The IN-SPACe Guidelines encourage the eventual transition of such operations under an Indian ITU filing, whenever feasible. Applicants who propose this approach within their initial application to IN-SPACe will receive priority consideration for authorization. This incentivizes the use of Indian orbital resources and streamlines future management within the established ITU framework. The Indian satellite communication market welcomes authorized non-Indian satellites, but with certain regulations. First, foreign operators must collaborate with an Indian entity through a subsidiary, joint venture, or similar partnership to offer satcom services within the country. IN-SPACe, the Indian space agency, grants authorization for these non-Indian satellites, valid for a maximum of five years or the satellite's operational lifespan, whichever comes first. Once authorized, operators can lease, sub-lease, sell, or resell their satellite capacity to service providers who then offer telecommunication or broadcasting services to end users. While service providers and end users don't require separate IN-SPACe authorization, they must comply with regulations set by relevant government bodies like the DoT or MIB. This approach ensures controlled access for foreign operators while providing flexibility for service providers and end users within the established regulatory framework.

2. Election Commission of India shares social media guidelines directing parties to take down deepfakes within 3 hours

On May 6, 2024, the Election Commission of India **("ECI")** has introduced comprehensive **guidelines** **("ECI guidelines")** for the responsible and ethical use of social media platforms during election periods. The ECI guidelines were formulated in response to complaints about the spread of edited and AI-manipulated deep fake videos that negatively portrayed political parties and politicians on social media. According to the ECI, the use of such manipulated and distorted content on social media has the potential to wrongfully influence voter opinions, deepen societal divisions, and erode trust in the electoral process. The ECI highlighted the dangerous scale of misinformation spread on social media, exacerbated by features like 'forwarding,' 're-sharing,' 're-posting,' and 're-tweeting,' which allow misinformation to propagate quickly and widely.

The salient features of the ECI guidelines stipulate the following directions for political parties:

- Prohibition ***from engaging in certain actions on social media to maintain the integrity of the electoral process***. Firstly, political parties are prohibited from disseminating any misinformation. This includes sharing any patently false, untrue, or misleading information, as well as synthetic content that has been created or modified to present false or distorted information as true. Secondly, parties must not impersonate other individuals, including political parties or their representatives, on social media. Additionally, the ECI emphasizes that political parties must refrain from posting or promoting content that is derogatory towards women, as such content is repugnant to the honor and dignity of women.
- Advice ***against using children in their campaigns***, adhering to the ECI's previous advisory on the matter.
- Prohibition ***from portraying violence against animals***, as such content is deemed unacceptable.
- Prohibition on usage of ***AI-based tools to distort information*** or spread falsehoods that could affect the fairness of elections. The use of deepfake audios or videos is also strictly prohibited unless it complies with existing regulations for a fair election process.
- Take down of ***any deepfake audios or videos*** within three hours of their appearance on social media platforms. They must also identify and warn the responsible individuals within their party.

- Report ***fake social media accounts*** impersonating their official handles to the respective social media platform and subsequently approach the Grievance Appellate Committee (GAC) under Rule 3A of the Information Technology Act.

By implementing the ECI guidelines, the ECI aims to mitigate the adverse effects of misinformation and unethical social media practices on the electoral process. Political parties are thus held to higher standards of accountability and transparency, ensuring that their use of social media during elections aligns with the principles of responsible and ethical conduct. The ECI's comprehensive approach not only addresses the immediate challenges posed by misinformation but also sets a precedent for future electoral conduct in the digital era. Through stringent monitoring and enforcement of these guidelines, the ECI seeks to uphold the sanctity of the electoral process and maintain public trust in democratic institutions.

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

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

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

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

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