VI

B&J | BHATT & JOSHI ASSOCIATES

EMERGING ISSUES:

OTT, SATELLITE & DIGITAL FUTURE

LEGAL DISCLAIMER

This booklet is published by Bhatt & Joshi Associates, Advocates & Solicitors, for general educational and informational purposes only. It does not constitute legal advice, and no attorney-client relationship is formed by reason of this publication. The content is based on primary legislative sources, official gazette notifications, regulatory instruments, and judicial decisions available as of the date of publication. Readers should not act on the basis of this publication without obtaining specific professional advice tailored to their circumstances. This publication complies with the Bar Council of India Rules on Standards of Professional Conduct and Etiquette.

TABLE OF CONTENTS

CHAPTER 1

OTT Communication Services: The Regulatory Question

1.1 Defining OTT Communication Services

Over-the-Top (OTT) communication services are digital services that provide voice, video, and messaging functionality to users over internet connections, substituting or supplementing the voice and messaging services traditionally provided by licensed telecommunications operators. The defining characteristic of OTT communication services — from a technical perspective — is that they ride on top of ("over the top of") the internet infrastructure provided by licensed broadband operators, without themselves operating telecommunications infrastructure or contributing directly to the cost of that infrastructure. From a user perspective, OTT communication services such as WhatsApp (with approximately 500 million active users in India), Telegram, Signal, Google Meet, Zoom, FaceTime, and Skype are functionally indistinguishable from traditional voice calls and SMS — yet they are provided outside the licensed telecommunications framework that imposes significant obligations (licence fees, spectrum charges, security conditions, quality of service requirements, and subscriber verification obligations) on their traditional counterparts.

The regulatory literature on OTT communication services distinguishes between several subcategories. OTT-A services (also termed "number-independent interpersonal communications services" under the EU Electronic Communications Code) include messaging applications that do not rely on telephone numbers for addressing — users are identified by username, email address, or phone number only for registration purposes, not for call routing. WhatsApp, Signal, Telegram, and Facebook Messenger fall into this category. OTT-B services include voice-over-internet services that do use telephone numbers for addressing and routing — services such as Skype Out (calling from a Skype account to a PSTN number), Google Voice, and Jio Call are examples. OTT-B services are more directly substitutable for traditional telephone calls and create stronger arguments for regulatory parity, since they use the same telephone number resources (E.164 numbers) as licensed operators. OTT-C services include enterprise unified communications platforms that provide communication services within a defined enterprise environment — Microsoft Teams, Slack, and Cisco Webex in their communication service aspects.

The economic significance of OTT communication services in India cannot be overstated. India is the world's largest market for WhatsApp by user count. The volume of messages, voice

calls, and video calls conducted over WhatsApp and similar OTT platforms vastly exceeds the corresponding volume over traditional SMS and voice channels. Reliance Jio's success in disrupting the Indian mobile market was substantially enabled by the fact that its subscribers' communication needs were met to a large extent by OTT services rather than traditional voice and SMS — making the economics of Jio's free-voice-call strategy sustainable even when the revenue per voice minute was near zero. The growth of OTT communication services has fundamentally altered the economics of the Indian telecom sector, reducing the revenue that licensed operators can generate from voice and SMS services while their infrastructure investment costs (particularly for the data networks that carry OTT traffic) continue to grow.

India's regulatory position on OTT communication services has been one of deliberate ambiguity — preserving the legislative flexibility to regulate while declining to exercise that flexibility at the present time. The Telecommunications Act, 2023's broad definition of "telecommunication services" encompasses OTT communication services within its scope, yet the government has administratively indicated that OTT services are not currently to be regulated under the Act. This preserved flexibility has been interpreted differently by different stakeholders: incumbent operators see it as an eventual commitment to regulatory parity; OTT providers see it as a pragmatic acknowledgement that OTT regulation is not technically feasible or commercially desirable; and consumer groups see it as a recognition that OTT communication services provide enormous consumer welfare benefits that would be reduced by regulatory burden. The eventual resolution of this regulatory ambiguity will be one of the most consequential telecommunications policy decisions of the decade.

1.2 The Level Playing Field Argument

The "level playing field" argument advanced by incumbent telecom operators for OTT regulation is the most commercially motivated and the most frequently articulated justification for regulatory intervention. The argument proceeds as follows: licensed telecom operators must comply with extensive and costly regulatory obligations including annual licence fees (as a percentage of AGR), spectrum usage charges, subscriber verification (KYC) requirements, lawful interception capability obligations, quality of service standards, coverage and rollout obligations, and consumer protection requirements. OTT communication services that provide functionally equivalent services to end-users are not subject to any of these obligations, creating a competitive advantage for OTT providers that is not based on genuine commercial or technological merit but on regulatory asymmetry. This asymmetry distorts competition in the communications services market, shifting revenue from regulated operators (who provide the infrastructure) to unregulated OTT providers (who free-ride on that infrastructure), ultimately

threatening the financial sustainability of network investment.

The level playing field argument, while commercially intuitive, is contested on several economic and regulatory grounds. First, OTT communication services and traditional telecom services are not simply substitutes — they are also complements. OTT services drive demand for mobile data, which is a primary revenue source for operators in the post-voice-revenue-decline era. An operator that deters OTT usage through regulatory restrictions (or through data charges that make OTT usage expensive) will also reduce demand for the mobile data services on which its revenue increasingly depends. Second, the regulatory obligations of licensed operators are not uniformly applicable to OTT services on a proportionate basis: some obligations (such as lawful interception, subscriber verification, and coverage requirements) have a genuine policy justification for OTT services; others (such as licence fees proportional to AGR) are primarily revenue measures for the government with less obvious policy justification for application to OTT services. Third, the regulatory framework for OTT services, if applied, must be designed to reflect the very different business models, cost structures, and geographic reach of OTT providers compared to licensed operators.

TRAI's extensive consultations on OTT regulation have generated analysis of the level playing field argument from both sides. In its 2015 Consultation Paper and subsequent engagement, TRAI acknowledged that there is a degree of regulatory asymmetry between OTT communication services and licensed telecom services, but declined at that stage to recommend OTT licensing. TRAI noted that many of the obligations imposed on licensed operators (particularly financial obligations such as licence fees and spectrum charges) were counterbalanced by the exclusive right to use licensed spectrum and to provide services that OTT providers cannot match without spectrum (particularly mobile coverage and mobility). The evolving TRAI position has been to move towards a tiered, proportionate framework in which certain specific obligations — particularly cybersecurity and lawful access obligations — might be applied to OTT communication services, while full regulatory parity (including licence fees and spectrum charges) would not be required.

The legal mechanism through which OTT regulation could be implemented — if the government chooses to do so — involves an important question under the Telecommunications Act, 2023. If OTT communication services are treated as "telecommunication services" under Section 2(22) of the Act, then OTT providers would be required to obtain authorisations under Section 3 of the Act. The conditions of such authorisations — which could include security conditions, consumer protection conditions, and potentially fee conditions — would be prescribed by the Central Government through rules. Alternatively, the government could create a specific

regulatory framework for OTT services through a class authorisation with bespoke conditions calibrated to the specific risk profile of OTT communication services — imposing cybersecurity, grievance redressal, and lawful access obligations while exempting OTT providers from the financial obligations (licence fees, spectrum charges) that are unique to spectrum-using operators.

1.3 International Approaches to OTT Regulation

The international regulatory landscape for OTT communication services reflects a wide range of approaches, from full regulatory parity (treating OTT services as equivalent to licensed telecom services for all regulatory purposes) to complete non-regulation (treating OTT services as internet applications with no telecom-specific obligations). The European Union's approach under the Electronic Communications Code (EECC), adopted in 2018, is the most sophisticated attempt to date to create a proportionate regulatory framework for OTT communication services. The EECC creates a new category of "number-independent interpersonal communications services" (NIICS) — which encompasses most messaging and voice-over-internet applications — and subjects them to a lighter set of regulatory obligations than traditional licensed services. NIICS providers must comply with: emergency services obligations (to the extent technically feasible); security requirements (including cybersecurity incident notification); and basic user rights provisions (under the Universal Service Directive). They are not required to obtain licences, pay licence fees, or comply with the full consumer protection framework applicable to traditional operators.

The EU approach has been implemented with varying degrees of effectiveness across EU member states, and its practical impact on major OTT providers — who are overwhelmingly US-based and subject to regulatory oversight in multiple EU member states simultaneously — has been mixed. The enforcement of NIICS obligations on providers headquartered outside the EU (such as WhatsApp, which is owned by Meta, a US company) has been the most challenging aspect of implementation. The EU's General Data Protection Regulation (GDPR), which applies to all data processing activities targeting EU residents regardless of where the data controller is located, has been more effectively enforced against major OTT providers than the EECC's specific communications obligations — reflecting both the more prescriptive nature of the GDPR's obligations and the more developed enforcement infrastructure around data protection compared to telecom regulation.

South Korea's regulatory framework for OTT services — which initially took a non-regulatory approach but then moved towards requiring large OTT providers to contribute to network infrastructure costs through a "network usage fee" arrangement — provides a different model.

South Korean legislators amended the Telecommunications Business Act in 2022 to require large content providers (including Google, Netflix, Apple, and others) to take reasonable measures to ensure stable provision of their services — effectively requiring them to negotiate commercial arrangements with ISPs for adequate network access rather than free-riding on network capacity. Whether this model — imposing network contribution obligations on OTT platforms rather than telecom-type licensing obligations — is appropriate for India's context is a question that TRAI and DoT will need to consider as the OTT regulation debate continues. India's large OTT platforms and the political sensitivity of any measure perceived as restricting free access to WhatsApp and other widely used services makes the regulatory design challenge particularly difficult.

1.4 Specific Regulatory Considerations for India

India's specific context creates a distinctive set of considerations for OTT regulation. First, the scale of OTT usage in India is among the highest in the world: India accounts for the largest WhatsApp user base globally, and Indian users are among the most data-intensive in the world. Any regulatory measure that increases the cost of OTT services, or that creates barriers to entry for new OTT providers, would affect hundreds of millions of users in ways that have both economic and social significance. Second, the digital divide in India means that OTT communication services play a particular role in enabling affordable communication for lower-income users who cannot afford traditional voice call charges: WhatsApp calling over a basic mobile data plan is significantly cheaper than traditional voice calls in many rural markets, enabling family communication, agricultural market information access, and small business communication for users who would otherwise be unable to afford these services. Third, India's large OTT platforms are predominantly operated by non-Indian companies (Meta, Alphabet, Apple, Microsoft), and any regulatory framework that imposes financial obligations on OTT providers would primarily affect these foreign companies — creating a potential trade friction dimension to what is primarily a domestic regulatory policy question.

The cybersecurity and lawful access dimensions of OTT regulation are particularly complex for India. Law enforcement agencies have repeatedly pressed for the ability to access messages sent through encrypted OTT communication services, arguing that terrorist recruitment, extremist content sharing, and coordination of criminal activities increasingly occurs through encrypted messaging platforms beyond the reach of lawful interception. The government's interest in traceability — the ability to identify the first originator of specific viral messages on encrypted platforms — is directly in tension with the end-to-end encryption architecture that is the primary security feature of leading OTT communication services. Any regulatory measure that compels

OTT providers to weaken their encryption or to build traceability into their systems must be assessed against: the Puttaswamy proportionality standard (is the measure necessary and proportionate to the legitimate aim?); the DPDPA's data protection framework (does the measure comply with subscriber privacy rights?); and the practical cybersecurity implications (does weakening encryption for law enforcement access also expose users to malicious actors?).

CHAPTER 2

Net Neutrality: India's Framework and Global Alignment

2.1 TRAI's 2016 Differential Pricing Regulations

India's net neutrality framework is anchored in TRAI's Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 — popularly known as the "net neutrality regulations" or the "zero-rating ban." These regulations, promulgated in February 2016, prohibit internet service providers (licensed telecom operators providing internet access) from offering or charging differentiated prices for data services based on the content of the data accessed, the specific applications used, the websites visited, or the communication services used. In plain terms, the regulations require that all internet traffic be treated equally for tariff purposes: a subscriber's data allowance is consumed equally regardless of whether they are using WhatsApp, Netflix, Google, Wikipedia, or any other online service.

The regulatory context for TRAI's 2016 regulations was the controversy over "zero-rating" schemes — commercial arrangements in which telecom operators charge subscribers zero data for accessing specific apps or websites (while charging for access to the rest of the internet). Facebook's Free Basics initiative (which offered free access to a curated set of internet services including Facebook, Wikipedia, and a limited set of health and educational services) and various operators' zero-rating arrangements (offering free access to specific streaming platforms, news sites, or e-commerce portals) were the direct triggers for the regulatory intervention. TRAI's consultation on these schemes generated over one million public submissions — the largest response to any regulatory consultation in India's history — with the overwhelming majority of submissions opposing zero-rating as a threat to the open internet. TRAI's Recommendations on Over-the-Top Services (2015) and the subsequent Recommendations on Net Neutrality (2015) recommended prohibiting content-discriminatory pricing, and these recommendations were implemented in the 2016 Regulations.

The legal basis for TRAI's 2016 Regulations is Section 11(2) of the TRAI Act, 1997, read with Section 36 (regulation-making power). The regulations were challenged before TDSAT by operators who argued that TRAI exceeded its jurisdiction in prohibiting commercial arrangements between operators and content providers, and that the regulations unreasonably restricted operators' commercial freedom. TDSAT upheld the regulations, and this decision was not further challenged before the Supreme Court. The stability of the 2016 Regulations over the years since their enactment — and the high degree of compliance achieved — reflects both the

strong public and judicial consensus in favour of net neutrality principles in India and the regulatory effectiveness of TRAI's enforcement approach (which focuses on monitoring and public disclosure of violations rather than heavy penalties for first-time infractions).

The Telecommunications Act, 2023 and its implementing rules will need to address the continued application of net neutrality principles in the 5G era. The 5G technology's capability for network slicing — creating differentiated logical networks with different quality-of-service characteristics — creates new potential for discriminatory treatment of internet traffic that must be assessed against the 2016 Regulations. TRAI's 2017 Recommendations on Net Neutrality provided some guidance on the application of net neutrality principles to network slicing: TRAI recommended that network slices used for licensed enterprise services (such as private 5G networks for specific industrial applications) are outside the scope of the net neutrality regulations (since they do not constitute internet access services as normally understood), while network slices providing internet access services to end-users must comply with net neutrality requirements in full. The boundary between "specialised services" (which may be offered with differentiated quality without violating net neutrality) and "internet access services" (which must comply with non-discrimination requirements) will be one of the defining regulatory questions of the 5G era.

2.2 The Non-Discriminatory Internet Access Regulations, 2018

Following TRAI's 2017 Recommendations on Net Neutrality, the Department of Telecommunications incorporated specific net neutrality provisions into the Unified Licence conditions through a licence amendment in 2018. The 2018 licence amendment — effectively incorporating the substance of TRAI's net neutrality recommendations into the licence framework — requires operators to treat all content, applications, and services equally while transmitting data over their networks. Specifically, operators are prohibited from: engaging in any form of discrimination in terms of treatment of content; either slowing down (throttling), blocking, or speeding up (prioritising) internet traffic based on the identity of the content provider or the nature of the content; or entering into arrangements with content providers for preferential treatment of their traffic on the operator's network.

The exceptions to the non-discrimination requirement in the 2018 licence amendment reflect the regulatory consensus on legitimate traffic management practices. Operators are permitted to manage their networks through: reasonable traffic management practices necessary to address congestion, security threats, or technical failures (provided these are proportionate and temporary); specialised services for specific network capabilities provided to users (such as managed VoIP services, IoT services, or private network services) that are technically distinct

from internet access services and are provided on the basis of commercial agreements with specific enterprises (not as part of the general internet access service). These exceptions preserve space for legitimate traffic engineering and for commercial specialised service offerings while maintaining the core principle that internet access services must be provided on a non-discriminatory basis.

2.3 Net Neutrality Enforcement: TRAI's Multi-Stakeholder Approach

TRAI's enforcement of net neutrality in India has relied on a multi-stakeholder approach that complements formal regulatory enforcement with transparency mechanisms, public accountability, and civil society monitoring. TRAI designated the Internet Society (ISOC) as the Multi-Stakeholder Body (MSB) for net neutrality monitoring, and worked with ISOC and other civil society organisations to develop a net neutrality monitoring and measurement framework. The framework uses crowd-sourced measurement tools (enabling users to test whether specific websites or services are being throttled or blocked by their operator) and technical measurement methodologies to generate data about the state of net neutrality compliance on Indian networks.

The multi-stakeholder monitoring approach has several advantages over pure regulatory enforcement. Crowd-sourced measurement data provides much broader coverage than TRAI's own monitoring capabilities, covering a wider range of networks, geographic locations, and times of day. Public transparency about net neutrality compliance — through published measurement data — creates reputational pressure on operators to maintain compliance, supplementing formal enforcement. The engagement of civil society organisations in monitoring creates a sustained public interest constituency for net neutrality enforcement that strengthens the regulatory framework beyond what government enforcement alone can achieve. The limitation of the approach is that it relies on the quality and scale of volunteer participation in measurement activities, and may miss systematic violations that are not detectable through end-user measurement tools.

CHAPTER 3

Satellite Broadband: Regulatory Framework

3.1 VSAT Services: Existing Framework

Very Small Aperture Terminal (VSAT) services — satellite-based broadband connectivity using geostationary orbit (GEO) satellites — have provided internet and data connectivity in India for commercial and government users since the 1990s. VSAT services are licensed by DoT under a separate VSAT licence category (and under the Unified Licence framework, as an additional service schedule to the UL). The VSAT sector in India has historically been small relative to the terrestrial broadband market, due to the significantly higher cost and lower performance (particularly the high latency inherent to GEO satellite communications, which at approximately 600 milliseconds round-trip-time is unsuitable for many interactive applications) compared to fibre and 4G/LTE broadband.

VSAT services in India require both a DoT licence for the provision of telecommunications services and a NOCC (Network Operations Centre and Control) licence from the Department of Space (through ISRO and IN-SPACe). The NOCC licensing requirement reflects the space segment dimension of VSAT services: the earth stations used in VSAT services communicate with satellite transponders, and the allocation and use of satellite capacity is subject to the jurisdiction of the Department of Space. The coordination between DoT (telecom services licensing) and the Department of Space (space segment authorization) is essential for VSAT operators and is one of the institutional complexities that the Telecommunications Act, 2023 and the developing space regulatory framework must address.

The pricing of VSAT services in India has historically been significantly higher than terrestrial broadband, reflecting both the high cost of satellite capacity and the regulatory overhead of VSAT licensing. TRAI has made several recommendations aimed at reducing the cost of VSAT services, including: reduction in the licence fee applicable to VSAT services; liberalisation of the frequency bands available for VSAT use; and the development of a framework for the integration of LEO satellite services into the VSAT regulatory framework. The entry of LEO satellite broadband services — with dramatically improved performance (lower latency, higher throughput) and potentially lower costs than GEO VSAT — will fundamentally transform the satellite broadband regulatory landscape, as discussed in Chapter 5.

3.2 The Spectrum Auction Requirement for Satellite Services

One of the most important regulatory questions for satellite broadband in India is whether the spectrum used for satellite services — particularly the Ku-band, Ka-band, and other frequency bands used for satellite communications — must be assigned through auction (consistent with the Supreme Court's 2G Spectrum Case holding and the First Schedule to the Telecommunications Act, 2023) or whether administrative allocation is permissible. The First Schedule to the 2023 Act includes "commercial satellite communication services" among the categories for which spectrum must be assigned by auction. This provision — if strictly applied — would require satellite broadband providers to bid for spectrum in an auction, potentially at costs that significantly affect the commercial viability of satellite broadband services in India.

The complication with applying the auction requirement to satellite communications spectrum is that satellite spectrum is fundamentally different from terrestrial mobile spectrum in several important ways. Satellite frequency bands are allocated globally by the ITU; the specific frequency assignments to individual satellites are coordinated through the ITU's satellite coordination procedure rather than through domestic auction. A country that auctions its satellite spectrum domestically in a manner that conflicts with ITU coordination procedures creates risks of harmful interference to satellite systems operated by other countries or organizations. The international framework for satellite spectrum coordination — through the ITU Radiocommunication Bureau's filing and coordination procedures — does not contemplate a domestic auction mechanism for satellite frequencies. India will need to develop an approach to satellite spectrum that meets the constitutional requirement for transparent commercial allocation while also being consistent with the international satellite spectrum coordination framework.

TRAI's recommendations on satellite spectrum allocation (issued in 2022) recommended an administrative allocation approach for satellite communications spectrum, with satellite operators required to pay market-determined pricing for their spectrum use rights through a fee-based mechanism rather than through a competitive auction. This approach — broadly consistent with the international practice for satellite spectrum allocation — was designed to avoid the WTO and ITU compatibility issues that a pure auction model would create. The recommendation has been contested by terrestrial mobile operators who argue that the absence of auction for satellite spectrum gives satellite broadband providers a competitive advantage in the race to serve India's unconnected rural markets. The regulatory resolution of this debate will significantly affect the commercial terms on which LEO satellite broadband services enter the Indian market.

3.3 Satellite Backhaul for Terrestrial Networks

Satellite backhaul — the use of satellite connectivity to connect remote base stations to the core network in areas where terrestrial fibre or microwave backhaul is unavailable — is an

important application of satellite technology in India's connectivity architecture. Remote and hilly geographic areas where terrestrial backhaul is technically or economically infeasible (including tribal areas, border regions, island territories, and disaster-prone areas) can be served by mobile networks using satellite backhaul, provided that the satellite latency is acceptable for the services provided. 5G's non-terrestrial network (NTN) component — which 3GPP specifications explicitly support — will enable integrated terrestrial and satellite connectivity, with mobile devices able to connect seamlessly to both ground-based base stations and satellite-based access points. The legal framework for NTN services — and specifically the question of whether satellite NTN services require separate satellite licensing in addition to the mobile operator's terrestrial licence — is an emerging regulatory question under the Telecommunications Act, 2023.

CHAPTER 4

IN-SPACe and the New Space Economy

4.1 The Policy Framework for Commercial Space

The Indian National Space Promotion and Authorisation Centre (IN-SPACe) was established by a government decision in June 2020 as the single-window authorisation body for private sector space activities in India. Prior to IN-SPACe's establishment, India's space sector was dominated by ISRO (the Indian Space Research Organisation), with private sector participation limited to specific supply chain roles (manufacturing of hardware under ISRO's direction). IN-SPACe's establishment was motivated by the recognition that the global commercial space industry was growing rapidly — driven by companies like SpaceX, OneWeb, Amazon, and Planet Labs — and that India needed a clear, efficient authorization framework to enable private Indian companies to participate in this commercial opportunity and to attract foreign space companies to establish operations in India. The New Space Policy, 2023 — formulated after extensive consultation — provides the policy framework within which IN-SPACe operates, emphasising the opening of the space sector to private investment while maintaining appropriate regulatory oversight for safety, security, and international treaty compliance.

IN-SPACe's mandate covers: the authorization of private sector entities (both Indian and foreign) to conduct space activities in India, including satellite launches, satellite operations, and space-related ground segment activities; the provision of access to ISRO facilities and expertise for private operators on commercial terms; the promotion of investment and innovation in India's commercial space sector; and the coordination of India's participation in international space activities and treaty frameworks. IN-SPACe operates under a regulatory framework that must balance India's obligations under international space law (particularly the Outer Space Treaty, 1967 and the Registration Convention, 1975) — which require states to authorize and continuously supervise national space activities — with the need to provide a commercially attractive and efficient authorization environment that encourages private investment.

The interaction between IN-SPACe's authorization of space activities and DoT's authorization of telecommunications services using satellite infrastructure is the key regulatory interface for the satellite broadband sector. An operator providing satellite broadband services in India requires: IN-SPACe authorization for the satellite (space segment) and associated operations; DoT authorization (under the Telecommunications Act, 2023) for the telecommunications services provided using the satellite; NOCC licensing from the Department

of Space for the network operations centre; and potentially WPC spectrum licensing for the earth station frequencies used in India. The development of a "one-stop" processing arrangement that allows satellite telecommunications operators to obtain all required authorizations through coordinated single-window processing — rather than through sequential applications to multiple agencies — is an important facilitation objective that the government has been pursuing but has not yet fully achieved.

4.2 Space Debris and Long-Term Sustainability

The rapid growth of satellite deployment — particularly by LEO broadband constellations deploying hundreds or thousands of satellites — creates significant concerns about space debris and long-term orbital sustainability. The near-Earth orbital environment, particularly the low-earth orbit region between 400 km and 1200 km altitude where most LEO broadband constellations operate, is subject to increasing congestion as more satellites are deployed. Satellite conjunctions (close approaches between satellites or between satellites and debris objects) are increasing in frequency, raising the risk of collisions that generate debris clouds threatening both the original satellite and other satellites in nearby orbits. The Kessler Syndrome — the scenario in which the density of objects in LEO becomes so high that collisions generate a cascade of further collisions, eventually rendering the orbital region unusable — is a long-term existential risk for the LEO-dependent digital economy.

India's regulatory framework for space debris mitigation — administered by IN-SPACe in coordination with ISRO's Space Situational Awareness programme — requires satellite operators to comply with the space debris mitigation guidelines of the Inter-Agency Space Debris Coordination Committee (IADC) and the UN guidelines on space debris mitigation. These guidelines require satellite operators to: design satellites to minimise debris generation; ensure passivation (removal of all stored energy) at the end of operational life; deorbit satellites from LEO within 25 years of end-of-mission; and avoid operational orbits that are particularly congested or sensitive (including the graveyard orbits used for decommissioned GEO satellites). The increasing ambition of LEO constellation operators has prompted proposals for more stringent deorbit requirements (5 years rather than 25 years) that India's regulatory framework will need to address.

CHAPTER 5

Low Earth Orbit Constellations in India

5.1 The Global LEO Landscape

The deployment of LEO broadband satellite constellations represents the most transformative development in satellite communications since the commercialization of GEO communications satellites in the 1970s. The fundamental technology innovation that makes LEO broadband commercially viable is the reduction in launch costs achieved by SpaceX's Falcon 9 and Falcon Heavy rockets (enabling large constellations through affordable mass launches) combined with the miniaturisation of satellite hardware (enabling high-performance satellites in the 200-500 kg class at a fraction of the cost of traditional GEO communications satellites). The result is a generation of broadband satellite systems — including SpaceX's Starlink (over 5,000 satellites deployed as of 2024, with plans for tens of thousands more), Amazon's Kuiper (2,000+ satellites planned), and Eutelsat OneWeb (648 satellites planned) — that can provide broadband internet access with latency in the range of 20-40 milliseconds (comparable to cable broadband) and throughput of 100+ Mbps per user beam, served by a constellation of satellites in low earth orbit.

The commercial implications of LEO broadband for India's connectivity landscape are profound. India has approximately 700 million people without reliable internet access, living primarily in rural and remote areas where terrestrial broadband (fibre or mobile 4G/5G) is commercially unviable or physically impossible to deploy. LEO broadband can serve these users at prices that, while currently higher than terrestrial broadband in covered areas, may become competitive over time as constellations scale and costs decline. The government's universal connectivity objectives — including the BharatNet programme and the Digital Bharat Nidhi's rural connectivity mandate — could potentially be achieved faster and more cost-effectively if LEO broadband is integrated into the connectivity architecture as a complementary technology to terrestrial networks, particularly for last-mile and backhaul connectivity in underserved areas.

India's LEO broadband regulatory framework is developing in the context of competing commercial interests and geopolitical considerations. Reliance Jio (through its Jio Space Technology subsidiary, using SES satellites and proprietary satellite technology) and Bharti Airtel (through its OneWeb shareholding and partnership) have significant domestic LEO broadband interests and would benefit from regulatory frameworks that protect their market position. Elon Musk's Starlink — which applied for DoT/IN-SPACe authorizations to provide services in India —

presents both a commercial competition to domestic players and a geopolitical consideration given its US ownership and the Indo-US strategic relationship. The government's approach to authorizing foreign-owned LEO broadband providers will reflect this complex intersection of commercial, geopolitical, and regulatory considerations.

5.2 Regulatory Challenges for LEO Services

The regulation of LEO broadband services in India involves several specific legal and regulatory challenges that do not arise for traditional GEO VSAT services. First, the dynamic nature of LEO constellations — with satellites constantly moving overhead and individual satellites having shorter operational lifetimes than GEO satellites — means that the space segment of a LEO broadband service is fundamentally different from the fixed satellite resources of a GEO VSAT service. The authorization framework must accommodate this dynamic character: authorizations for LEO services cannot be tied to specific satellite positions (as GEO authorizations are) but must cover the constellation as a whole. Second, the global footprint of LEO constellations — which, by design, provide coverage over all or most of the Earth's surface — means that the same satellite infrastructure simultaneously serves users in multiple countries, creating jurisdictional complexity for regulatory oversight, lawful interception, and data protection compliance.

The lawful interception requirement for LEO broadband services is a particularly sensitive issue. The Telecommunications Act, 2023's security conditions (including the requirement for lawful interception capability) are designed for terrestrial networks where the physical infrastructure is located in India and can be technically compelled to implement interception. LEO broadband services use space-based infrastructure (the satellite constellation) that is physically located outside India and is operated by companies potentially headquartered outside India. Compelling a foreign-operated satellite constellation to implement India-specific lawful interception — on the same terms as domestically operated telecom networks — involves both legal complexity (the jurisdictional basis for extraterritorial regulatory requirements) and technical complexity (LEO satellites do not have the same LI infrastructure as terrestrial base stations). The development of a technically and legally workable framework for lawful access to LEO broadband communications is one of the most challenging regulatory design problems in India's satellite broadband governance.

CHAPTER 6

5G: Legal Dimensions Beyond Spectrum

6.1 Network Slicing and Regulatory Classification

5G's network slicing capability — enabling the creation of multiple virtual network instances on a single physical 5G infrastructure, each with customised quality-of-service characteristics — creates novel regulatory classification challenges that the existing telecommunications regulatory framework was not designed to address. The regulatory classification of a network slice determines which regulatory obligations apply: if a slice providing dedicated industrial IoT connectivity for a specific factory campus is classified as a licensed telecommunications service, the enterprise customer using it may require authorisation under Section 3 of the Telecommunications Act, 2023; if it is classified as a managed service sold by the licensed operator to the enterprise customer (analogous to a corporate VPN or managed WAN service), it may fall within the operator's existing authorisation without requiring separate enterprise authorisation.

TRAI's engagement with network slicing has addressed the net neutrality dimensions: as discussed in Chapter 2, TRAI has recommended that network slices used for specialised non-internet services (such as factory automation, V2X communications, or healthcare monitoring) are outside the scope of the net neutrality framework, while slices providing internet access to end-users must comply with net neutrality requirements. This distinction — between "internet access service slices" (subject to net neutrality) and "specialised service slices" (not subject to net neutrality) — provides a workable framework in principle but requires clear criteria for distinguishing between the two categories in practice. The criteria should be based on the technical and commercial characteristics of the service (is it genuinely a distinct managed service with specific quality parameters, or is it simply internet access with priority queuing?) rather than on the label applied by the operator.

The legal framework for 5G network sharing — specifically the question of whether sharing a 5G network slice between two operators (MOCN sharing) requires a separate spectrum sharing agreement in addition to the commercial network sharing agreement — is an important operational question for operators building shared 5G infrastructure. Under DoT's existing spectrum sharing framework (described in Booklet III), MOCN sharing requires prior DoT approval and compliance with spectrum cap requirements. In the context of 5G network slicing, the same physical 5G deployment may support both shared access service slices (where

multiple operators serve their respective retail subscribers using a shared RAN) and dedicated enterprise service slices (where a single operator provides a private network service to a specific enterprise customer). The regulatory treatment of these different slice types on the same physical infrastructure — and the question of whether each type of sharing requires separate regulatory approval — needs clarification in the 2023 Act's implementing rules.

6.2 5G for Critical Infrastructure: Legal Issues

The use of 5G networks for critical infrastructure applications — including smart grid automation, water and gas utility management, transportation systems, and emergency communications — creates specific legal issues around the security, resilience, and availability obligations applicable to 5G services. Critical infrastructure operators in these sectors have both high requirements for network performance (ultra-reliability, sub-millisecond latency, guaranteed bandwidth) and high sensitivity to service disruptions. The use of commercial 5G networks for critical infrastructure applications may be appropriate for some use cases but creates regulatory complexity: the licensed operator's commercial network is subject to the regulatory framework of the Telecommunications Act, 2023, while the critical infrastructure application is subject to the sector-specific regulatory framework of the critical infrastructure sector (power, water, transportation, etc.). The appropriate allocation of responsibility for service availability guarantees — between the telecom operator and the critical infrastructure operator — needs to be clearly defined in service level agreements and in the regulatory framework.

Emergency communications — the communications systems used by police, fire, ambulance, and disaster management agencies — are a specific application of 5G for critical infrastructure where the regulatory stakes are highest. India's emergency communications infrastructure currently relies on a combination of dedicated radio networks (using TETRA and similar narrowband technologies) and commercial mobile networks. The development of a 5G-based broadband emergency communications network — analogous to FirstNet in the United States or the Emergency Services Network (ESN) in the United Kingdom — would provide emergency services with access to the high-bandwidth communications capabilities (including video surveillance, real-time mapping, and data-intensive incident management tools) that 5G enables. The legal framework for a national 5G emergency communications network — including the funding mechanism (government-funded or commercially-operated), the spectrum allocation (dedicated public safety spectrum or commercial spectrum under priority access arrangements), and the governance structure — is an important policy question that the 2023 Act's framework must accommodate.

CHAPTER 7

Internet of Things: Legal and Regulatory Framework

7.1 IoT Connectivity Services and Licensing

The Internet of Things (IoT) — encompassing connected devices from smart meters and industrial sensors to consumer electronics and connected vehicles — is one of the fastest-growing applications of telecommunications technology and will account for an increasing share of the device connections (if not the revenue) in India's telecommunications market over the coming decade. The legal and regulatory framework applicable to IoT connectivity services in India is complex because IoT encompasses a vast range of use cases with very different technical, commercial, and regulatory characteristics. A connected cattle tracking device in rural India using NB-IoT technology, a smart electricity meter using PLC (power line communications), and an autonomous vehicle using C-V2X cellular vehicle-to-everything technology all involve "connected devices" but have almost nothing else in common from a regulatory perspective.

DoT's Machine-to-Machine (M2M) and IoT policy, articulated through the National Telecom M2M Roadmap (2015) and subsequent policy documents, provides the framework for IoT connectivity regulation. The M2M Roadmap established requirements for IoT devices and connectivity services including: mandatory use of domestically manufactured SIM cards for cellular-connected IoT devices; compliance with security standards for IoT devices connecting to telecommunications networks; and a registration framework for M2M service providers. The cellular IoT connectivity provided by licensed operators (using NB-IoT and LTE-M network capabilities) falls within the operator's existing access service authorisation; the provision of M2M platform services (middleware, application enablement, and data management services for IoT deployments) may require a separate M2M service provider registration.

The security framework for IoT devices connecting to Indian telecommunications networks is a growing regulatory concern. IoT devices have historically been designed with minimal security features, creating large numbers of insecure connected devices that can be exploited for various attacks. India's security framework for IoT devices — currently based on CERT-In guidelines and the IT Act's broad computer security provisions — lacks the specific, binding technical standards applicable to the European Union's Cyber Resilience Act (which mandates minimum cybersecurity requirements for all digitally connected products sold in the EU) or the UK's Product Security and Telecommunications Infrastructure Act, 2022 (which requires manufacturers to publish security update policies and prohibit default passwords). The

development of India-specific mandatory IoT security standards — aligned with international standards such as the ETSI EN 303 645 Consumer IoT security standard — is a regulatory priority that the Telecommunications Act, 2023's security standards framework should address through rules.

7.2 Connected and Autonomous Vehicles

Connected and autonomous vehicles (CAVs) represent one of the most strategically important IoT applications from a telecommunications regulatory perspective. CAVs require reliable, low-latency wireless connectivity for: vehicle-to-vehicle (V2V) communication (enabling collision avoidance and cooperative driving); vehicle-to-infrastructure (V2I) communication (enabling traffic signal coordination, road condition updates, and toll collection); vehicle-to-pedestrian (V2P) communication (enabling awareness of vulnerable road users); and vehicle-to-network (V2N) communication (enabling real-time traffic management, software updates, and infotainment services). The spectrum requirements for CAV communications — specifically, the allocation of spectrum in the 5.9 GHz band for dedicated short-range communications (DSRC) or the use of cellular technologies (C-V2X using 5G NR) — is a policy question that DoT and the Ministry of Road Transport and Highways must jointly resolve.

The legal framework for CAV communications involves a complex intersection of telecommunications law (governing the connectivity technologies), automotive safety regulation (governing vehicle systems), road traffic law (governing the rules applicable to autonomous driving), and product liability law (governing responsibility for accidents involving CAVs). The Telecommunications Act, 2023's framework is relevant to CAV communications through its spectrum management provisions (spectrum allocation for V2X communications), its critical infrastructure protection provisions (CAV communications networks may qualify as critical telecom infrastructure given their safety-critical role), and its security standards provisions (the security of V2X communications is essential to prevent spoofing attacks that could cause accidents or traffic disruptions). Practitioners advising automotive manufacturers, technology providers, and infrastructure operators in the CAV space must navigate all these intersecting legal frameworks simultaneously.

CHAPTER 8

Platform Regulation and Digital Markets

8.1 The Platform Economy and Telecom

The major digital platforms — including Alphabet (Google), Meta (Facebook/Instagram/WhatsApp), Amazon, Apple, and their Indian counterparts (Reliance Jio Platforms, Zomato, Swiggy, Flipkart) — operate at the intersection of the telecommunications sector and the broader digital economy. Their relationship with the telecom sector is multidimensional: as the primary sources of data traffic (streaming, social media, and app store downloads account for the majority of mobile data consumption in India); as providers of OTT communication services that substitute for traditional telecom voice and messaging; as participants in the infrastructure stack (through content delivery networks, data centres, and potentially their own access infrastructure); and as powerful commercial partners (or competitors) for telecom operators in the provision of services to consumers.

The regulatory framework for digital platforms in India involves multiple statutes and regulators. The IT Act's intermediary liability framework (Section 79 and the Intermediary Guidelines, 2021) applies to social media platforms and OTT platforms as "intermediaries." The Competition Act, 2002 and the Competition Commission of India (CCI) apply to anti-competitive conduct and abusive behaviour by dominant platforms — CCI has taken enforcement action against several major platforms in recent years, including proceedings against Google (for abuse of dominance in the Android ecosystem) and proceedings against Meta (for WhatsApp's privacy policy). The DPDPA, 2023 applies to the data processing activities of all platforms serving Indian users. And the proposed Digital Competition Bill — if enacted — would establish an ex ante framework for regulating "systematically significant digital enterprises" (analogous to the EU's Digital Markets Act gatekeeper designation).

The telecom regulatory framework's interface with platform regulation is primarily through TRAI's mandate to regulate interconnection, tariffs, and consumer protection in the communications sector. As OTT platforms increasingly provide communications services that were previously the exclusive domain of licensed operators, TRAI's regulatory mandate — designed for a world of licensed operators and wireline/wireless networks — must evolve to address the platform-network boundary. The question of whether platforms that provide communications services over licensed networks can or should be subject to TRAI regulation (in addition to the IT Act's intermediary regulation and competition law) is a fundamental

architectural question for India's digital regulatory framework that has not yet been definitively resolved.

8.2 The Digital Markets Bill and Telecom Implications

The proposed Digital Competition Bill for India — developed by the Ministry of Corporate Affairs following the recommendations of the Committee on Digital Competition Law (CDCL) — seeks to establish a framework for ex ante regulation of major digital platforms with the intent of preventing anti-competitive conduct before it occurs (rather than the traditional competition law approach of remedying anti-competitive conduct after it has caused harm). The Bill proposes to designate platforms meeting specified thresholds (in terms of users, revenue, or market capitalization) as "Systemically Significant Digital Enterprises" (SSDEs) and to impose specific obligations on SSDEs including: non-discrimination requirements; data portability mandates; interoperability requirements; and restrictions on self-preferencing (promoting the platform's own products and services at the expense of competing products). The implications of the Digital Competition Bill for the telecommunications sector are significant if major telecom operators' digital platform offerings (including Jio's JioMeet, JioCinema, JioMart, and similar services) qualify for SSDE designation — which is possible given the scale of Jio's digital services platform.

The interoperability requirements in the proposed Digital Competition Bill are of particular relevance to the telecom and OTT sectors. Interoperability requirements — requiring dominant messaging platforms to enable users of different messaging services to communicate with each other — are analogous to the interconnection requirements that TRAI imposes on telecom operators, and are based on a similar rationale: preventing network effects from entrenching the dominance of incumbents at the expense of competitive entry. The EU's Digital Markets Act includes interoperability requirements for gatekeeper messaging platforms; the technical implementation of these requirements (using protocols such as Signal's encryption protocol or the Matrix open messaging protocol) is being developed in the EU context and will provide relevant technical precedent for India's implementation. Telecom operators, as existing providers of messaging services (through their carrier messaging platforms) and as potential beneficiaries of messaging interoperability (if major OTT platforms are required to interoperate with carrier messaging), have a significant commercial interest in the outcome of the interoperability policy debate.

CHAPTER 9

Digital Public Infrastructure and UPI

9.1 Telecom's Role in DPI

India's Digital Public Infrastructure (DPI) ecosystem — comprising Aadhaar (identity), UPI (payments), DigiLocker (document sharing), and emerging additions such as Ayushman Bharat Health Account (ABHA) — is built on telecommunications connectivity as its foundational layer. Without reliable, affordable, widely accessible telecommunications connectivity, the DPI ecosystem cannot function: Aadhaar-based biometric authentication requires internet connectivity for real-time verification; UPI transactions require reliable mobile connectivity for generating and receiving payment requests; DigiLocker requires connectivity for document access and sharing. The DPI ecosystem's success — India processes more real-time digital payments than any other country in the world, accounting for approximately 46% of global real-time payment volume — is therefore directly dependent on the quality and reach of India's telecommunications infrastructure.

The legal framework for the telecommunications infrastructure underlying the DPI ecosystem involves the Telecommunications Act, 2023 (for the connectivity layer), the DPDPA (for the data protection obligations associated with DPI data processing), the Aadhaar Act, 2016 (for Aadhaar-based authentication used in telecom subscriber verification and many DPI applications), and the Payment and Settlement Systems Act, 2007 (for UPI and other payment infrastructure). Telecom operators occupy a unique position in this framework: they are both regulatory subjects (required to comply with the Telecommunications Act) and infrastructure providers for the DPI ecosystem (providing the connectivity over which DPI transactions occur). The government's promotion of digital payments, digital identity, and digital services depends on telecom operators providing connectivity of adequate quality, coverage, and affordability.

The intersection of the Aadhaar framework and the telecom KYC framework has been legally complex since the Aadhaar Act's passage. The Supreme Court's 2019 Aadhaar judgment (Puttaswamy v. UoI) struck down the use of Aadhaar-based e-KYC by private entities — including telecom operators — as unconstitutional, holding that the Aadhaar Act's framework for private entity use of Aadhaar was not constitutionally proportionate. The government's response was the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Amendment Act, 2019, which created a voluntary Aadhaar-based e-KYC framework for the private sector with specific consent requirements. Telecom operators use the voluntary e-KYC

framework for subscriber verification, which requires individual subscriber consent for Aadhaar-based authentication. The legal complexity of balancing Aadhaar-based efficiency in subscriber verification with the constitutional privacy requirements is an ongoing compliance challenge for the telecom sector.

CHAPTER 10

Universal Service: BharatNet and Beyond

10.1 BharatNet: Legal and Implementation Framework

BharatNet — India's national broadband infrastructure programme for rural gram panchayats — is the largest rural broadband deployment programme in the world by geographic scope and target coverage. The programme was originally conceived as the National Optical Fibre Network (NOFN) in 2011, with a target of connecting all 2.5 lakh gram panchayats with 100 Mbps broadband connectivity. The programme was renamed BharatNet in 2015 and restructured multiple times in response to implementation challenges — including slow progress in civil works (trenching and cable laying), inadequate last-mile connectivity, and challenges in ensuring the operational sustainability of deployed infrastructure. The Digital Bharat Nidhi (formerly USOF) finances BharatNet through contributions from licensed telecom operators, providing the funding stream for infrastructure deployment, maintenance, and operations.

The legal framework for BharatNet involves a complex multi-stakeholder structure. Bharat Broadband Network Limited (BBNL), a special purpose vehicle operating under BSNL (following BBNL's merger into BSNL in 2023), manages the core BharatNet infrastructure. State-level entities — through State-level SPVs or direct state agency implementation — manage state-specific components in many states. Private contractors engage in civil works, installation, and last-mile connectivity deployment. ISPs and telecom operators use BharatNet infrastructure on commercial terms to provide retail broadband services to end-users. The legal frameworks governing each of these relationships include: BBNL's MoU with DoT (governing BBNL's mandate and funding); state implementation agreements (governing state agency responsibilities and federal funding); contract agreements with private infrastructure contractors; and the BharatNet open access framework (governing commercial terms for ISPs and operators using BharatNet infrastructure).

The open access obligation — requiring BBNL and state entities to provide BharatNet infrastructure access to all licensed ISPs and operators on non-discriminatory, commercially reasonable terms — is essential for the programme's intended role as a shared national digital backbone. Without open access, BharatNet could become a vehicle for BSNL's competitive advantage in rural broadband, undermining the competitive market development that serves consumers' long-term interests. The open access framework must strike a balance between ensuring that access terms are commercially viable (providing BharatNet with the revenue to

maintain and expand its infrastructure) and ensuring that access prices are low enough to incentivize ISPs and operators to build the last-mile connectivity services that convert BharatNet infrastructure into end-user broadband services.

10.2 The Digital Bharat Nidhi's Expanded Mandate

The renaming of the Universal Service Obligation Fund (USOF) as the Digital Bharat Nidhi under the Telecommunications Act, 2023 reflects a deliberate policy choice to expand the fund's mandate beyond its traditional focus on universal basic telephony access to a broader mandate encompassing the full range of digital connectivity and digital public infrastructure objectives. Section 28 of the 2023 Act provides that the Digital Bharat Nidhi may be applied for the purposes of: providing access to telecommunications services; providing broadband connectivity in rural and remote areas; developing and promoting India's technology and innovation ecosystem for telecommunications; facilitating R&D; in telecommunications; and such other purposes as may be prescribed. This expanded mandate — in particular the inclusion of R&D; and technology development — significantly broadens the scope of USOF/DBN activity beyond infrastructure financing to encompass the full digital development agenda.

The governance of the Digital Bharat Nidhi — the processes by which programme priorities are determined, projects are evaluated and sanctioned, and implementation is monitored — is as important as the statutory mandate in determining the fund's effectiveness. Historically, USOF programmes have been criticized for slow sanction processes, inadequate project monitoring, and insufficient accountability for outcomes (connection counts rather than service quality and sustainability). The 2023 Act's framework does not prescribe detailed governance arrangements for the DBN, leaving these to rules. The development of a robust, outcomes-oriented governance framework for the DBN — with clear program evaluation criteria, competitive procurement processes, independent implementation monitoring, and transparent reporting — is an important component of realizing the fund's potential as an instrument for India's digital development.

CHAPTER 11

Competition Law in Digital Telecom Markets

11.1 The Competition Commission and the Telecom Sector

The Competition Commission of India (CCI) has been an increasingly active presence in the telecommunications and digital markets sectors, exercising its jurisdiction under the Competition Act, 2002 to address anti-competitive agreements and abuse of dominant position by telecom operators and digital platforms. CCI's concurrent jurisdiction with TRAI (for economic regulation of the telecom sector) and with TDSAT (for dispute adjudication) creates potential for overlapping regulatory oversight and for inconsistent decisions across the two institutional frameworks. The Supreme Court has generally resolved this potential conflict in favour of maintaining concurrent jurisdiction — CCI can investigate and order remedies for competition law violations by telecom operators even where TRAI has concurrent regulatory jurisdiction — though the Court has also emphasised the need for coordination and consistency between the two regulatory frameworks.

CCI's investigations in the telecom sector have addressed: roaming charges (CCI closed an investigation into alleged anti-competitive coordination among operators on roaming charges, finding no evidence of a cartel); call drops (CCI investigated whether operators had colluded in failing to invest in network quality improvements); SIM card blocking (investigations into alleged market division through agreed geographic boundaries for network investment); and infrastructure sharing arrangements (assessment of whether active infrastructure sharing between competitors reduces competition). CCI's most important ongoing telecom-adjacent investigation concerns the telecommunications equipment market — specifically, whether Ericsson, Nokia, and other network equipment vendors have abused their dominant position in the market for telecom network equipment by charging excessive prices and imposing restrictive licensing terms.

The Telecom Equipment Manufacturers Association (TEMA) and individual operators have made submissions to CCI regarding competition concerns in the telecom equipment supply chain, including the vertical integration of major equipment vendors (who supply both infrastructure equipment and managed services), the exclusive relationships between vendors and operators that may foreclose the market to alternative suppliers, and the patent royalty arrangements for standards-essential patents (SEPs) that govern access to the core technology underlying all cellular communications. The SEP licensing question — whether Ericsson, Nokia,

Qualcomm, and other patent holders charge fair, reasonable, and non-discriminatory (FRAND) royalties for access to their patented technologies — has been one of the most complex competition law questions in the global telecom industry and has generated both CCI investigations and IP court proceedings in India.

11.2 Market Concentration and 5G Investment

India's mobile market has consolidated from six or seven major private operators in the mid-2010s to three operators (Reliance Jio, Bharti Airtel, and Vi/Vodafone Idea) following the Jio disruption and the subsequent exit of several operators (including Aircel, RCOM, and Telenor) and the merger of Vodafone India and Idea Cellular. This concentration creates a three-player oligopoly in which competitive dynamics are significantly different from those in a more fragmented market. CCI's assessment of the current market structure — and specifically whether the three-player market provides sufficient competitive intensity to protect consumer interests in pricing and quality — is a key regulatory question. TRAI's ongoing monitoring of competition in the mobile sector, and CCI's jurisdiction over any further consolidation, provides the institutional framework for managing market concentration concerns.

The interplay between market concentration and 5G investment presents a complex regulatory balance. On one hand, excessive market fragmentation — many small operators each with insufficient scale to finance 5G network investment — may result in inadequate 5G deployment and poor quality of service. On the other hand, excessive market concentration — a two or three-player oligopoly with limited competitive pressure — may result in higher prices, reduced quality, and insufficient innovation. The three-player market India currently has may be at a reasonable competitive equilibrium, but the financial challenges facing Vi (Vodafone Idea) — which, if they lead to Vi's market exit or a further merger, would reduce the market to a duopoly — are a significant concern for competition and consumer welfare. The government's extraordinary financial support for Vi (through the equity conversion of AGR dues and spectrum charges) reflects the recognition that a two-player market would be seriously damaging to competition and consumer welfare.

CHAPTER 12

Taxation of Digital Telecom and OTT Services

12.1 GST on Telecom Services

The taxation of telecommunications services in India underwent a fundamental transformation with the introduction of the Goods and Services Tax (GST) in July 2017. Under GST, telecommunications services are classified under the category of "services" subject to 18% GST. This replaces the pre-GST regime of service tax (15%) and various state-level levies. The GST rate on telecommunications services — among the highest rates in the GST framework — reflects the high revenue significance of the sector and the government's reliance on telecoms-derived tax revenue. The interaction between GST on telecom services and the licence fee framework (which also represents a significant government revenue take from the sector) means that the total fiscal burden on the telecom sector is substantial, and has been identified by industry associations as a factor constraining investment in network infrastructure.

Several specific GST classification issues have generated litigation and regulatory guidance in the telecom context. The classification of roaming services (whether interstate roaming constitutes an inter-state supply attracting IGST or an intra-state supply attracting CGST + SGST, depending on the place of supply rules) was a significant compliance issue in the early years of GST implementation. The treatment of interconnection services between operators (whether these are B2B services subject to the reverse charge mechanism) created compliance complexity for operators managing large volumes of inter-operator settlements. The GST treatment of bundled services — packages combining voice, data, OTT subscriptions, and device financing — required careful analysis of the "principal supply" rules for composite supplies. And the question of whether roaming services provided to foreign tourists visiting India (inbound roaming) constitute exports of services (exempt from GST) or taxable domestic supplies has been addressed in various advance rulings with some inconsistency.

12.2 Equalisation Levy and OTT Taxation

The taxation of digital services provided by non-resident technology companies to Indian users — including OTT video streaming, cloud services, and OTT communication services provided by foreign companies — has been addressed through the Equalisation Levy framework introduced in the Finance Act, 2016 (as extended by the Finance Act, 2020). The 6% Equalisation Levy on online advertising services purchased from non-resident providers, and the

2% expanded Equalisation Levy on e-commerce supply and services (introduced in 2020), apply to revenue earned by non-resident digital businesses from Indian users without a physical presence in India. The expanded Equalisation Levy has been contested by the United States as discriminatory against US technology companies, and its future has been linked to the global OECD/G20 Pillar One framework for digital economy taxation.

The interaction between the Equalisation Levy and telecom operators' tax obligations is relevant because operators often serve as collection points for digital service payments: when an Indian subscriber purchases an OTT subscription (Netflix, YouTube Premium, Spotify) and pays through their telecom operator's billing system, the operator may be treated as the collection agent for the subscription payment and may have obligations under the Equalisation Levy framework. The legal analysis of whether operators collecting payments for foreign OTT services are themselves subject to Equalisation Levy obligations — or whether the obligation falls on the OTT provider directly — has been addressed in various tax authority communications with differing results depending on the commercial structure of the payment collection arrangement.

CHAPTER 13

AI in Telecom: Regulatory Implications

13.1 AI Applications in Telecommunications

Artificial intelligence is transforming the telecommunications industry across the full stack of network operations, customer service, fraud detection, and product innovation. Network planning and optimization — using AI to analyze traffic patterns, predict congestion, and optimize radio resource allocation across thousands of base stations — is among the most commercially impactful applications. AI-powered customer service — chatbots, virtual assistants, and intelligent call routing — reduces operating costs while improving customer experience. AI-based fraud detection — identifying unusual usage patterns indicative of SIM cloning, international revenue share fraud, and subscription fraud — reduces revenue losses that historically amounted to a significant fraction of operator revenue. Predictive maintenance — using AI to identify network equipment likely to fail before failure occurs — reduces network downtime and maintenance costs.

The 5G era is enabling new AI applications in telecommunications that go beyond traditional use cases. AI-native RAN (Radio Access Network) — in which AI algorithms control the physical layer radio transmission in real-time, optimizing beam forming, interference management, and spectrum use — promises to significantly improve spectral efficiency and network capacity. Open RAN architecture, promoted by the O-RAN Alliance, enables AI-based network intelligence to be deployed across disaggregated, multi-vendor RAN components in ways that are not possible in proprietary, monolithic RAN architectures. These technical innovations have regulatory implications: AI-based network management decisions that affect service quality (including coverage, latency, and throughput) may need to be subject to regulatory transparency and audit requirements to ensure that AI-driven network management does not result in discriminatory treatment of specific users or applications in violation of net neutrality principles.

TRAI's 2023 consultation paper on AI and machine learning in telecommunications invited stakeholder views on: the regulatory framework applicable to AI applications in telecom; whether AI-based network management decisions should be subject to explainability and transparency requirements; the accountability framework for AI-driven decisions that affect consumer welfare (such as AI-based credit scoring for post-paid subscriptions or AI-based churn prediction used for discriminatory retention offers); and the application of data protection law to the subscriber data used for AI training and inference. The recommendations that emerge from this consultation

will be an important contribution to the emerging global regulatory framework for AI in telecommunications — a framework that many regulators are developing simultaneously without the benefit of a well-established international consensus.

13.2 The EU AI Act and India's Regulatory Gap

The European Union's Artificial Intelligence Act (AI Act) — adopted in 2024 as the world's first comprehensive AI regulation — provides a risk-based framework for AI systems that is directly relevant to telecommunications applications. The AI Act classifies AI systems into four risk categories: prohibited AI (systems with unacceptable risks, such as social scoring by governments); high-risk AI (systems requiring conformity assessments, including AI systems used in critical infrastructure, employment, education, and law enforcement); limited-risk AI (systems subject to transparency obligations, including chatbots and deepfake technology); and minimal-risk AI (systems not subject to mandatory requirements). AI systems used in critical telecommunications infrastructure — such as AI-based network management, security monitoring, and fraud detection systems — would likely be classified as high-risk under the AI Act framework, requiring operators deploying such systems to conduct conformity assessments, maintain technical documentation, and implement human oversight mechanisms.

India does not yet have an AI-specific regulatory framework analogous to the EU AI Act. The National Strategy for Artificial Intelligence (NSAI) and the draft National AI Policy articulate India's aspirations for AI development and governance, but do not constitute binding regulatory requirements. The DPDPA, 2023 provides a data protection framework applicable to AI training and inference involving personal data, but does not specifically address AI safety or liability for AI-driven decisions. MEITY's draft Advisory on Responsible Development and Deployment of AI (2024) provides guidance for AI developers and deployers, but is non-binding. The regulatory gap between India's aspirational AI policy framework and the binding regulatory requirements being developed in the EU and other jurisdictions creates both a competitive advantage (lower regulatory burden may accelerate AI adoption in India) and a risk (the absence of clear AI liability rules may discourage enterprise adoption of AI in risk-sensitive applications). The Telecommunications Act, 2023's security standards framework provides some basis for addressing AI-specific security requirements in telecom networks, but a more comprehensive AI governance framework for the sector will eventually be needed.

CHAPTER 14

Quantum Communications and the Next Frontier

14.1 Quantum Technology and Telecommunications

Quantum communications — the application of quantum mechanical principles to telecommunications, particularly for information security purposes — represent the long-term frontier of telecommunications technology with profound implications for the security frameworks built around classical cryptography. The most commercially advanced quantum communications technology is quantum key distribution (QKD), which uses the quantum properties of photons (specifically, the no-cloning theorem and the principle that measurement of a quantum state disturbs that state) to enable two parties to establish a provably secure cryptographic key that cannot be intercepted without detection. QKD is fundamentally different from classical encryption: rather than relying on the computational difficulty of mathematical problems (which could in principle be solved by a sufficiently powerful classical or quantum computer), QKD's security is based on the laws of quantum physics, which are not breakable by computational means.

The National Mission on Quantum Technologies and Applications (NM-QTA), launched under India's Union Budget 2020-21 with an allocation of Rs. 8000 crore, includes quantum communications as one of its key technology areas. The mission funds research and development in quantum cryptography, quantum sensing, and quantum computing, with the intention of developing both indigenous quantum technology capabilities and the human resources needed for India's quantum technology ecosystem. The Department of Telecommunications is a key participant in the NM-QTA, particularly in the context of developing quantum secure communications networks for government and critical infrastructure applications. A quantum communication network connecting New Delhi with key government facilities and critical infrastructure nodes would provide security guarantees against quantum computer-based attacks on India's most sensitive communications.

The regulatory implications of quantum communications for the Telecommunications Act, 2023 framework are not yet developed but will become increasingly significant as QKD and other quantum communications technologies transition from research laboratories to operational deployments. Key regulatory questions will include: should QKD links be subject to the same licensing requirements as classical optical fibre links? How should the interception framework under Section 24 of the 2023 Act apply to quantum-secured communications (where interception

is physically impossible without detection, making lawful interception in the traditional sense technically infeasible)? What security standards should apply to quantum communications infrastructure? And what spectrum considerations apply to free-space quantum optical communications (which may use optical wavelengths outside the traditional telecom bands)?

14.2 Post-Quantum Cryptography: Preparing the Telecom Sector

While QKD represents the offensive use of quantum principles for communications security, post-quantum cryptography (PQC) addresses the defensive challenge of protecting existing classical communications systems from attack by quantum computers. Current classical public-key cryptography systems — including RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange — are theoretically vulnerable to attacks by sufficiently powerful quantum computers running Shor's algorithm. The timeline for quantum computers capable of breaking current cryptographic systems is uncertain (current estimates range from 10 to 25+ years), but the "harvest now, decrypt later" threat — in which adversaries collect encrypted data today with the intent of decrypting it once quantum computing capability becomes available — means that long-lived sensitive data (including classified government communications, sensitive financial data, and critical infrastructure control data) is potentially at risk today.

The U.S. National Institute of Standards and Technology (NIST) published its first set of Post-Quantum Cryptographic Algorithm Standards in 2024, providing algorithm specifications for three PQC algorithms (CRYSTALS-Kyber for key encapsulation, CRYSTALS-Dilithium and FALCON for digital signatures) that are resistant to quantum computer attacks. These standards provide the technical foundation for transitioning telecommunications security frameworks from classical cryptography to quantum-resistant cryptography. India's telecommunications sector — through the TEC, C-DoT, and CERT-In — is engaged in assessing the PQC transition requirements and developing a roadmap for migrating critical network security functions (including network authentication, key management, and secure communications between network elements) to PQC algorithms. The Telecommunications Act, 2023's security standards framework provides the regulatory basis for requiring operators to implement PQC standards as they are finalised and operationalised.

CHAPTER 15

The Future Regulatory Architecture for Digital India

15.1 Convergence Regulation: The Long-Term Trajectory

The convergence of telecommunications, broadcasting, and internet services — all increasingly delivered over the same internet protocol infrastructure — has been the defining structural trend of the information and communications technology sector for two decades. The regulatory architecture that governs this converged landscape in India — with separate regulatory frameworks for telecommunications (under the Telecommunications Act, 2023 and the TRAI Act, 1997), broadcasting (under the Cable Television Networks Regulation Act, 1995 and the Prasar Bharati Act, 1990), and online content (under the IT Act and the Intermediary Guidelines) — was designed for a world in which these services were delivered over distinct, non-interchangeable infrastructures. The regulatory fragmentation creates inconsistency (the same content delivered over different networks may be subject to different rules), gaps (content delivered over the internet may fall between the regulatory frameworks applicable to broadcasting and telecommunications), and compliance costs (operators providing converged services must comply with multiple overlapping regulatory frameworks simultaneously).

The long-term regulatory trajectory for digital India should move towards convergence regulation — a single regulatory framework (or at least a coherent, consistent multi-statute framework) that addresses all electronic communications and digital services without regard to the delivery technology. The EU's Electronic Communications Code (EECC) provides a model of convergence regulation for the network layer: all electronic communications services, regardless of technology, are subject to the same basic regulatory framework. For the content layer, convergence regulation is more challenging, given the very different policy considerations applicable to broadcast content (which is delivered to mass audiences without individual selection or control) and internet content (which is accessed individually and with a high degree of user agency). India's proposed Broadcasting Services (Regulation) Bill — which seeks to extend content regulation to online broadcasting platforms — is a step towards convergence regulation of the content layer, though its exact scope and approach continue to be debated.

The institutional implications of convergence regulation are significant. A truly converged regulatory framework would require either a single converged regulator (combining TRAI's telecommunications and broadcasting economic regulation functions with MeitY's internet intermediary oversight functions and MIB's content regulation functions) or at minimum a formal

mechanism for coordinating the separate regulators' activities across the converged service landscape. The establishment of a Digital Regulatory Coordination Council — a forum bringing together TRAI, CCI, MeitY, MIB, and other relevant regulators for coordinated policy development and enforcement — would be a significant institutional improvement on the current fragmented approach, even in the absence of full institutional convergence.

15.2 The Rights-Based Approach to Digital Governance

The long-term sustainability of India's digital governance framework depends on its alignment with the fundamental rights framework established by the Puttaswamy, Anuradha Bhasin, and related Supreme Court decisions. The rights-based approach to digital governance — recognising privacy, freedom of expression, economic opportunity, and access to information as constitutional rights that digital regulation must respect and protect — provides a framework of constraints and aspirations within which the Telecommunications Act, 2023, the DPDPA, the IT Act, and all other digital governance legislation must operate. Regulatory decisions that fail to satisfy the proportionality standard — that are not based on a specific legal provision, that do not pursue a legitimate aim, or that impose restrictions disproportionate to the aim pursued — are constitutionally vulnerable, as the growing body of High Court and Supreme Court jurisprudence on internet shutdowns and surveillance demonstrates.

The rights-based approach also provides positive regulatory imperatives: the State has an obligation not merely to refrain from violating digital rights but to create conditions in which all citizens can effectively exercise those rights. Universal internet access — ensuring that every Indian has access to affordable, reliable, high-speed broadband — is a constitutional imperative under the right to information, the right to education, and the right to practise a profession: in the digital age, these rights cannot be effectively exercised without internet access. The Digital Bharat Nidhi's connectivity mandate, the BharatNet programme, and the government's PM-WANI and rural broadband initiatives reflect this rights-based affirmative obligation. The Telecommunications Act, 2023's universal connectivity provisions — and the effective implementation of those provisions — are constitutional imperatives as well as policy goals.

15.3 India's Role in Global Digital Governance

India's influence in global digital governance is growing commensurate with its position as the world's most populous democracy, the world's largest mobile market by subscriber count (and one of the largest by data traffic), and a significant global technology power through its IT services sector, its thriving start-up ecosystem, and its public digital infrastructure achievements. India's success with UPI — adopted as a model by multiple countries globally and supported by

NPCI International's international deployment — demonstrates the potential for India's digital governance models to influence global practice. India's advocacy for a "Digital Public Infrastructure" approach to digital development — open, interoperable, publicly funded digital platforms as an alternative to proprietary commercial platform dominance — has gained significant international traction, particularly in the context of the G20 and the ITU's development agenda.

The Telecommunications Act, 2023's framework — as the statutory foundation for India's telecommunications regulatory architecture — must be designed with both domestic effectiveness and international credibility in mind. A regulatory framework that is internationally recognised as providing adequate protections for privacy, freedom of expression, and competitive market development will support India's integration into the global digital economy, attract foreign investment in digital infrastructure, and enhance India's credibility as a proponent of balanced, rights-respecting digital governance. A framework that is perceived internationally as primarily serving surveillance interests, restricting competitive entry, or protecting incumbents at the expense of innovation will have the opposite effect — reducing investment, limiting connectivity, and undermining India's aspirations as a global digital leader.

The five preceding booklets in this series — on the Telecommunications Act, 2023 (Booklet I), TRAI and the Regulatory Architecture (Booklet II), Licensing, Spectrum and Infrastructure (Booklet III), TDSAT Jurisprudence (Booklet IV), and Cybersecurity, Data Protection and National Security (Booklet V) — have provided the detailed legal and regulatory analysis needed to understand and navigate the full complexity of India's telecommunications legal framework. This sixth booklet has addressed the emerging and future dimensions of that framework: OTT, satellite, 5G, IoT, platform regulation, AI, quantum communications, and the long-term trajectory towards convergence regulation. Together, these six booklets constitute a comprehensive reference for practitioners, policymakers, investors, and scholars engaged with one of the most dynamic and consequential regulatory environments in the global economy — the legal framework governing India's digital future.

SUPPLEMENTARY NOTE A

Advanced Analysis: OTT, Platform and Digital Economy Law

A.1 OTT Regulation: Comparative Framework

The global experience with OTT communication service regulation provides important lessons for India's ongoing policy development in this area. The European Union's approach under the Electronic Communications Code (EECC), adopted in 2018 and implemented in EU member states by 2020, created a three-tier regulatory framework: traditional licensed operators (subject to full sector regulation); "number-based interpersonal communications services" (NIICS) that use telephone numbers for addressing, such as Skype Out (subject to a lighter set of obligations including emergency service access); and "number-independent interpersonal communications services" (NIICS-NI) such as WhatsApp and Telegram (subject to the lightest obligations, primarily limited to security and emergency access requirements). This tiered approach allows regulatory requirements to be calibrated to the degree of substitutability between OTT services and traditional licensed services, applying heavier obligations where substitution is more direct (number-based services) and lighter obligations where the difference from traditional services is more pronounced (number-independent services).

The implementation of the EU's EECC OTT framework has revealed several practical challenges that India should take note of. First, enforcement extraterritorially against major OTT providers headquartered outside the EU has been complex: national regulatory authorities (NRAs) in EU member states have faced jurisdictional challenges in applying OTT-specific obligations to services provided by US-based companies without a significant physical presence in the specific member state. The EECC addresses this by applying the framework to services targeting users in a member state regardless of where the provider is established, but enforcement against non-compliant foreign OTT providers relies on market access pressures (the threat of being required to comply or losing market access) rather than direct regulatory action. Second, the practical definition of the boundary between "number-independent" and "number-based" services has been complicated by the evolution of OTT services: apps like WhatsApp use phone numbers for account registration and user identification, even though call routing between WhatsApp users does not use the public telephone numbering plan. The classification of WhatsApp as NIICS-NI (lighter obligations) or NIICS (heavier obligations) has been resolved differently by different EU member states. India's regulatory framework will need to address similar definitional questions.

The South Korean model — which imposes "network usage fees" on large content providers and mandates stable service quality obligations — reflects a different regulatory philosophy: rather than applying telecom-type obligations to OTT providers, it requires OTT providers to internalise some of the network cost externalities they create. Korea's Telecommunications Business Act amendment (2022) requiring large content providers to take "reasonable

measures" for stable service quality is effectively a network contribution requirement disguised as a quality obligation — it requires OTT providers with large traffic volumes (Netflix, Google, Apple, etc.) to enter into commercial arrangements with telecom operators for adequate network capacity. The legal validity of this approach under WTO trade law (specifically, whether it discriminates against foreign OTT providers in violation of the MFN and national treatment obligations) is contested; several US content providers have filed WTO complaints against South Korea's network usage fee framework. India's awareness of these legal constraints will be important in designing any network contribution obligation for OTT providers.

The developing-country perspective on OTT regulation — which reflects both the consumer welfare benefits of OTT services (particularly for lower-income users) and the infrastructure investment concerns of telecom operators — is an important dimension of the debate that India, as the world's largest developing-country mobile market, is well-positioned to articulate in international regulatory forums. India's advocacy for a framework that: preserves the consumer welfare benefits of affordable OTT communication services; creates a proportionate obligation framework for OTT services on cybersecurity and lawful access matters (without imposing financial burdens that would raise the cost of OTT services); and addresses the infrastructure investment funding challenge through approaches that do not require OTT services to be licensed as telecom services — would reflect a pragmatic, consumer-oriented approach consistent with India's digital development objectives and with the constitutional right to access the internet established in Anuradha Bhasin.

A.2 5G and the New Service Economy

5G technology is enabling a new category of telecommunications services that go far beyond the smartphone-centric mobile broadband model of 4G. The three core service categories defined by ITU-R for IMT-2020 (5G) — eMBB (enhanced Mobile Broadband), uRLLC (ultra-Reliable Low-Latency Communications), and mMTC (massive Machine-Type Communications) — each enable distinct commercial applications with very different regulatory implications. eMBB — providing very high data rates for consumer applications including 4K/8K video streaming, immersive AR/VR experiences, and high-speed hotspot connectivity — is an evolution of existing mobile broadband services and falls straightforwardly within the existing access service authorisation framework. uRLLC — providing extreme reliability (five-nines or higher availability) and very low latency (below 1 millisecond) for mission-critical applications including industrial automation, remote surgery, and vehicle-to-infrastructure communications — creates new regulatory questions about the quality of service obligations applicable to life-safety and mission-critical services provided over commercial 5G networks. mMTC — providing

connectivity for billions of IoT devices with extremely low power consumption and the ability to serve very dense device deployments — creates new questions about the licensing framework applicable to entities deploying large-scale IoT connectivity services that do not fit neatly within the existing access service or internet service provider categories.

The regulatory framework for uRLLC services — 5G services providing ultra-reliable, low-latency connectivity for mission-critical applications — requires careful attention to the quality-of-service obligations and liability implications of mission-critical services. When a 5G network slice providing uRLLC connectivity for a robotic surgical system fails, the consequences may be catastrophic — patient harm or death resulting from the communication failure. The allocation of legal responsibility between the 5G network operator (who provided the connectivity), the medical device manufacturer (who designed the robotic system), the hospital (who procured and operated the system), and the surgeon (who performed the procedure) in the event of such a failure is a complex product liability question that Indian tort law and medical negligence law are not yet fully equipped to address. The development of liability rules and insurance frameworks for mission-critical 5G services — specifying the responsibilities of each actor in the value chain and the compensation mechanisms available to persons harmed by communication failures — is an important regulatory gap that must be addressed as uRLLC services are commercially deployed.

The mMTC dimension of 5G — providing connectivity for massive IoT deployments — connects directly to the regulatory framework for IoT devices discussed in Chapter 7 of this booklet. As 5G enables the connection of billions of devices at unprecedented density and scale, the regulatory questions about IoT security, data privacy, spectrum management, and emergency deactivation capabilities become correspondingly more urgent. The Telecommunications Act, 2023's framework for authorisations, security standards, and spectrum management provides a statutory basis for addressing these questions, but the implementing rules must provide specific guidance on the regulatory treatment of large-scale mMTC deployments — including the authorisation requirements for IoT platform operators, the security standards for connected devices, and the spectrum management framework for the frequency bands (including NB-IoT and LTE-M bands) used for IoT connectivity.

A.3 The Future of BharatNet

BharatNet's future trajectory — whether it will achieve its transformative connectivity objectives or remain a programme defined more by its aspirations than its achievements — will be determined by how effectively the government addresses the structural challenges that have limited its progress so far. The most fundamental structural challenge is the last-mile connectivity

gap: BharatNet has been reasonably successful in laying optical fibre to gram panchayat headquarters, but far less successful in translating this backbone connectivity into actual broadband services for rural households and businesses. The gap between fibre deployment (to gram panchayats) and service availability (to individual users) reflects: the absence of business models that make last-mile retail broadband commercially viable in low-income rural markets; the limited competitive participation of private ISPs in using BharatNet infrastructure (partly due to the open access framework's commercial terms being insufficiently attractive); the inadequate maintenance of deployed infrastructure (leading to high rates of fibre cuts and outages that undermine service reliability); and the limited demand for broadband services in areas where digital literacy is low and devices are expensive.

The Digital Bharat Nidhi's potential role in addressing the last-mile challenge is significant if its expanded mandate is used creatively. DBN funding could support: subsidies for consumer devices (smartphones and Wi-Fi routers) in BharatNet-served areas, reducing the device access barrier for potential broadband subscribers; digital literacy training programmes, increasing the demand for broadband services by building the skills and awareness needed to use digital services effectively; community broadband cooperatives, providing a local organisational model for sustainable last-mile broadband provision in low-density rural areas; and innovation grants for companies developing last-mile business models that are commercially sustainable in rural markets without ongoing subsidy. The combination of infrastructure investment (BharatNet fibre to gram panchayats) with demand-side support (device subsidies, digital literacy, and community broadband models) is more likely to achieve the transformative connectivity outcomes that India's development ambitions require than infrastructure investment alone.

The integration of satellite broadband into the BharatNet architecture — using LEO satellite connectivity to serve gram panchayats not reachable by fibre within commercially viable timelines, and as backup connectivity for fibre-connected gram panchayats during outages — is a policy option that the government has been actively considering. The Digital Bharat Nidhi framework provides a mechanism for funding satellite backhaul for gram panchayats in difficult terrain (hills, forests, islands, and flood-prone areas) where fibre deployment is technically challenging or economically prohibitive. The integration of satellite and terrestrial connectivity in a coherent rural broadband architecture — with clear technical standards for interoperability, fair commercial terms for satellite access to the BharatNet network, and appropriate regulatory oversight of the combined system — requires a holistic approach to rural connectivity planning that goes beyond the traditional boundaries between the telecom regulatory framework (governing terrestrial connectivity) and the space regulatory framework (governing satellite

connectivity).

A.4 The Digital Economy: Taxation, Investment and Trade

The taxation of digital economy activities — including OTT services, e-commerce, cloud computing, and digital advertising — is a global policy challenge that India has been at the forefront of addressing. India's Equalisation Levy (6% on online advertising, 2% on e-commerce supply of goods and services by non-resident operators) was one of the first unilateral digital economy tax measures globally, predating the OECD's Pillar One and Pillar Two framework by several years. The Equalisation Levy has generated significant revenue (estimated at thousands of crore rupees annually from major US technology companies operating in India) and has been a factor in US trade pressure on India through the Section 301 process under US trade law. The convergence between India's domestic Equalisation Levy framework and the OECD/G20 two-pillar framework for digital economy taxation is an important ongoing policy and legal process: India has committed to withdrawing the Equalisation Levy upon the implementation of the OECD framework, but the specific timing and the commercial terms of the transition are still being negotiated.

Foreign direct investment in India's digital economy — including in telecommunications infrastructure, OTT platforms, fintech, and e-commerce — is governed by the FDI policy administered by DPIIT under the FEMA framework. The current FDI policy allows 100% FDI in telecommunications services and infrastructure under the automatic route, subject to security conditions. E-commerce and fintech are subject to more complex and evolving FDI frameworks that address concerns about market dominance, data localisation, and the commercial practices of large e-commerce operators. The interaction between FDI policy and telecom regulation creates specific considerations for foreign-owned telecom operators and OTT providers entering the Indian market: foreign ownership in a telecom authorisation holder triggers the security conditions applicable to foreign-owned telecom infrastructure (including requirements for domestic directors, restrictions on foreign nationals in security-sensitive roles, and enhanced compliance with national security agency requirements for network access).

India's digital economy trade commitments — both under existing FTAs and under future trade negotiations — are an important constraint on domestic regulatory choices in the telecom and OTT sectors. The TRIPS Agreement's provisions on intellectual property (including software copyright and database rights) affect the regulatory framework for digital services. The WTO's General Agreement on Trade in Services (GATS) telecommunications commitments — under which India has made specific commitments on market access for telecommunications services — constrain India's ability to impose discriminatory licensing requirements on foreign telecom

operators. India's position in ongoing WTO trade negotiations on digital economy issues — including the Joint Statement Initiative on Electronic Commerce and negotiations on rules for digital trade — will shape the international regulatory framework within which India's domestic digital economy regulation must operate. Practitioners advising foreign companies seeking market access to India's digital economy, or Indian companies seeking market access in foreign digital markets, must navigate both India's domestic regulatory framework and India's international trade commitments simultaneously.

SUPPLEMENTARY NOTE B

Digital Future: Legal Analysis

B.1 The Metaverse and Telecommunications Regulation

The metaverse — a network of interconnected, immersive three-dimensional virtual environments accessible through extended reality (XR) technologies including virtual reality (VR) headsets, augmented reality (AR) glasses, and mixed reality platforms — represents one of the most significant potential use cases for advanced telecommunications technologies, particularly 5G's ultra-low-latency connectivity and edge computing capabilities. The immersive experiences that characterise the metaverse require data rates, latency levels, and processing capabilities far beyond what previous generations of telecommunications technology could provide: high-fidelity VR environments require multi-Gbps data rates and sub-20ms latency to avoid motion sickness; real-time AR overlays on physical environments require sub-10ms latency and edge computing resources located close to the user. 5G networks with edge computing infrastructure — deployed as Multi-Access Edge Computing (MEC) nodes at or near base stations — are positioned as the enabling infrastructure for mass-market metaverse applications.

The regulatory implications of the metaverse for India's telecommunications framework are multifaceted. First, the metaverse's requirements for extremely high data rates and low latency create a demand pull for 5G network densification and edge computing deployment that will drive significant additional infrastructure investment. The right-of-way framework, the small cell deployment facilitation provisions, and the spectrum management framework of the Telecommunications Act, 2023 will all be tested by the infrastructure requirements of a mature metaverse. Second, the identity and data implications of the metaverse — persistent digital identities tied to physical persons, vast quantities of biometric data (including full-body motion capture and facial expression data) collected to animate avatars, and detailed records of metaverse activities — create data protection challenges that go significantly beyond the

DPDPA's current design, which was developed primarily with the web 2.0 data model in mind. Third, the metaverse's virtual economies (including NFT-based digital asset markets, virtual currency systems, and platform-based income opportunities for digital creators) create taxation, financial regulation, and consumer protection questions that will test the boundaries of existing regulatory frameworks.

The social and psychological dimensions of the metaverse — the potential for immersive virtual environments to create addiction, social isolation, or harm to vulnerable users including children — create regulatory questions that go beyond the technical telecommunications framework but that telecommunications regulators may be drawn into given their oversight of the connectivity layer through which metaverse experiences are delivered. The age verification requirements of the DPDPA, the prohibition on harmful processing of children's data, and the consumer protection provisions of the Telecommunications Act's authorisation framework may all be relevant to addressing metaverse-related consumer protection concerns. The regulatory framework for the metaverse in India is embryonic, and the telecommunications sector's role in shaping that framework — through constructive engagement in government consultations, industry standards bodies, and international regulatory discussions — will be important in ensuring that the framework facilitates innovation while protecting the interests of Indian metaverse users.

B.2 Autonomous Vehicles and 5G: Legal Interface

India's emerging autonomous vehicle (AV) ecosystem — which includes significant government investment in connected vehicle infrastructure, the development of domestic AV technology companies, and pilot deployments in specific geographic contexts — creates a direct interface between the telecommunications regulatory framework and the automotive regulatory framework. AVs require telecommunications connectivity for several categories of function: safety-critical real-time communication between vehicles and between vehicles and infrastructure (V2X), requiring ultra-reliable, low-latency 5G connectivity; software over the air (OTA) updates for AV software systems, requiring secure, high-bandwidth connectivity; telemetry data transmission from vehicles to fleet management systems, requiring persistent, low-cost connectivity; and emergency services communication in the event of accidents or malfunctions, requiring reliable connectivity to emergency call centres.

The spectrum allocation for V2X communications in India — specifically the allocation of dedicated short-range communications (DSRC) spectrum in the 5.9 GHz band or the adaptation of C-V2X using 5G NR in licensed mobile bands — has not yet been resolved as a matter of telecommunications policy. The Ministry of Road Transport and Highways (MoRTH) and DoT are

engaged in consultation about the appropriate V2X spectrum framework, with the choice between dedicated ITS (Intelligent Transportation Systems) spectrum and C-V2X in licensed mobile spectrum having significant implications for both the telecommunications regulatory framework (spectrum allocation, interference management, and technical standards for base station and vehicle-side equipment) and the automotive regulatory framework (type approval requirements for V2X-equipped vehicles, safety standards for V2X-dependent driving functions, and liability frameworks for accidents involving V2X system failures). The resolution of these interdepartmental questions through a comprehensive connected vehicle regulatory framework — jointly developed by DoT, MoRTH, and other relevant ministries — is a priority for enabling India's ambitious connected vehicle deployment plans.

The liability framework for accidents involving autonomous vehicles is one of the most complex and unresolved legal questions in the AV regulatory domain globally, and India's product liability, motor vehicles liability, and telecommunications liability frameworks will all be potentially relevant in specific accident scenarios. Where an AV accident is caused by a failure of the 5G V2X connectivity system (for example, a failure to transmit a collision warning that would have enabled the vehicle's autonomous driving system to take evasive action), the telecommunications operator's liability — under contract with the vehicle operator and potentially in tort to persons injured in the accident — is a significant legal exposure. The standard of care applicable to a telecommunications operator providing V2X connectivity for safety-critical AV functions is higher than the standard for general mobile broadband provision: the safety consequences of connectivity failure are direct and potentially catastrophic, and the operator's knowledge of the safety-critical nature of the connectivity (from the commercial contract and from the technical specifications of the V2X service) makes the heightened duty of care legally sustainable. The development of specific service level agreements, liability caps, and force majeure provisions for V2X connectivity services — calibrated to the safety-critical nature of the application — is an important area for legal practice and regulatory guidance.

B.3 Web3 and Blockchain in Telecom

Web3 — the vision of a decentralised, blockchain-enabled internet in which users own and control their digital identities, data, and assets rather than entrusting them to centralised platform operators — has specific applications in the telecommunications sector that are beginning to move from concept to commercial deployment. Blockchain-based identity systems — providing a tamper-evident, portable digital identity that subscribers can use across multiple telecommunications operators and digital services without repeated KYC verification — could significantly reduce the cost and friction of subscriber verification while improving security and

privacy. A subscriber's digital identity credentials — verified once by a trusted authority using Aadhaar-based e-KYC or equivalent — could be stored in a blockchain-based decentralised identity (DID) system and presented to any participating operator or service provider for instant, zero-knowledge verification without exposing the subscriber's underlying identity documents. This "verify once, use anywhere" model for digital identity in telecommunications could transform the subscriber onboarding process while also improving compliance with DPDPA's data minimisation principles (since operators would receive only the verification confirmation they need, not the full subscriber identity data).

Blockchain-based telecom roaming settlement — using smart contracts to automate the clearing and settlement of international roaming charges between operators — is one of the most commercially advanced blockchain applications in telecommunications. The traditional roaming settlement process involves complex multi-party billing and settlement arrangements, with settlement cycles of several months and significant disputes about billing accuracy. Smart contract-based settlement — automatically executing and settling roaming transactions in near real-time based on verifiable data from both operators' billing systems — can reduce settlement delays from months to minutes, reduce settlement disputes by providing a transparent, agreed settlement basis, and lower the operational costs of roaming settlement for both operators. The GSMA's blockchain settlement pilots (including the work of the GSMA Blockchain Taskforce) have demonstrated the technical feasibility of blockchain-based roaming settlement and are informing the development of commercial implementations.

B.4 Spectrum Management in the 6G Era

The development of 6G technology — expected to begin commercial deployment in the early 2030s in leading markets — is shaping the long-term agenda for spectrum management globally, and India's preparation for 6G will be one of the most important telecommunications policy priorities of the coming decade. 6G is expected to use spectrum across a much wider range of frequency bands than previous generations, including: sub-6 GHz bands (already used for 4G and 5G) for coverage; mmWave bands (already partially used for 5G) for high-capacity urban deployments; and new sub-terahertz (sub-THz) bands in the range of 100-300 GHz for extreme-capacity short-range applications. The sub-THz bands are largely unexplored territory for commercial telecommunications, with very limited propagation range (a few tens to hundreds of metres) but extraordinary capacity (potentially terabits per second throughput in dense deployments). Their commercial applications will likely be concentrated in specific scenarios — factory floors, entertainment venues, data centre interconnects — where the extreme capacity justifies the deployment complexity.

India's preparation for 6G spectrum management involves multiple dimensions. At the research level, C-DoT, TEC, IITs, and other Indian research institutions are participating in 6G technology development through the government's India 6G Vision programme, contributing to the design of the radio interface and network architecture that will underpin India's 6G spectrum requirements. At the standards level, India's participation in 3GPP (which is developing the 6G specifications under the IMT-2030 framework) and ITU-R (which is developing the IMT-2030 vision and spectrum requirements) is essential for ensuring that India's spectrum usage patterns and deployment scenarios are reflected in the global 6G standards. At the regulatory level, the WPC Wing and TRAI must develop India's spectrum management framework for 6G — covering NFAP allocations, auction frameworks, assignment conditions, and sharing arrangements — in advance of the commercial deployment timeframe. The lead time required for spectrum planning (from WRC allocation to national frequency plan update to auction design to commercial deployment) means that India must begin its 6G spectrum planning work now, even though commercial deployment is still a decade away.

The legal and regulatory framework for 6G will need to address several novel challenges that do not arise in the current 4G/5G framework. The integration of terrestrial and non-terrestrial networks (NTN) in 6G — with seamless connectivity between ground-based base stations, low earth orbit satellites, and high altitude platform stations (HAPS) — creates regulatory jurisdiction questions about which national authority regulates which component of the integrated 6G system. The use of AI for real-time network management in 6G — including AI-driven spectrum sharing, interference management, and resource allocation — requires a regulatory framework that addresses the use of AI in safety-critical network functions and that ensures accountability for AI-driven network management decisions. And the extreme capabilities of 6G (sub-millisecond latency, terabit capacity, near-universal connectivity) will enable applications that current regulatory frameworks were not designed to address — from holographic telepresence to ubiquitous environmental sensing — requiring early regulatory engagement to ensure that the framework keeps pace with technology.

B.5 Green Telecom: Environmental Regulation

The environmental impact of telecommunications infrastructure — particularly the energy consumption of mobile networks, data centres, and the manufacturing of billions of connected devices — is an emerging dimension of telecom regulation that the Telecommunications Act, 2023 and its successor frameworks will need to address more explicitly. India's telecommunications sector is a significant energy consumer: mobile base stations consume large quantities of electricity (a significant portion of which is generated from diesel generators in

areas without reliable grid power, creating both cost and carbon emissions concerns), and the rapid growth of 5G (which requires more densely deployed base stations and edge computing resources than 4G) will increase the sector's energy footprint. The development of sustainable telecommunications infrastructure — powered by renewable energy, designed for energy efficiency, and incorporating circular economy principles in equipment manufacturing and end-of-life management — is both an environmental imperative and a commercial opportunity.

The regulatory framework for green telecommunications in India is nascent but developing. TRAI's consultation on Sustainable Telecommunications (2021) was an early engagement with the environmental dimensions of telecom regulation, addressing energy efficiency standards for network equipment, renewable energy mandates for telecom infrastructure, and the reduction of hazardous materials in telecommunications equipment. The Environment Protection Act, 1986 and the E-Waste (Management) Rules, 2022 address the end-of-life management of electronic waste (including discarded telecommunications equipment), requiring manufacturers and operators to manage e-waste responsibly through authorised recyclers. The Bureau of Energy Efficiency's standards and labelling programme — which prescribes energy efficiency requirements for certain categories of electrical and electronic equipment — may be extended to include telecommunications infrastructure equipment as energy efficiency becomes a more prominent regulatory priority.

The energy security dimension of telecommunications infrastructure — ensuring that telecom networks remain operational during power grid failures, natural disasters, or deliberate attacks on power infrastructure — intersects with the environmental agenda in important ways. Base stations powered primarily by renewable energy (solar and wind) with battery storage are both more environmentally sustainable and more resilient than base stations dependent on grid power and diesel backup: they can continue operating during grid outages without the cost and environmental impact of diesel generation. The development of hybrid renewable-diesel-battery power systems for remote base stations — supported by Digital Bharat Nidhi funding for rural connectivity — would improve both the environmental sustainability and the resilience of rural telecommunications infrastructure. The Telecommunications Act, 2023's framework for critical infrastructure protection includes an implicit mandate to ensure the resilience of telecommunications power supply — a mandate that aligns with the environmental objective of transitioning to renewable energy.

SUPPLEMENTARY NOTE C

Digital Economy Law: Emerging Issues

C.1 The Creator Economy and Telecom

The "creator economy" — the ecosystem of individual content creators, influencers, podcasters, live streamers, and short-form video producers who monetise their digital content through platform advertising revenue, paid subscriptions, fan support, and brand partnerships — has become one of the most economically significant applications of mobile internet connectivity in India. India has one of the world's largest creator economies by number of active creators, driven by the accessibility of video production (via smartphones), the scale of social media platforms (YouTube, Instagram, and homegrown platforms like ShareChat), and the monetisation opportunities available through these platforms. The telecommunications infrastructure that enables the creator economy — mobile broadband connectivity for uploading and streaming video content, edge computing for real-time live streaming, and CDN (Content Delivery Network) infrastructure for low-latency content delivery — is directly relevant to the telecommunications regulatory framework.

The regulatory implications of the creator economy for the telecommunications sector include several specific dimensions. Net neutrality enforcement is relevant to ensuring that creator content can be delivered to audiences without discriminatory treatment: an operator that prioritises the delivery of content from major studios or streaming platforms (which can afford premium CDN arrangements) over the delivery of content from independent creators (who rely on best-effort internet delivery) would violate the non-discrimination principle of TRAI's 2016 regulations. The copyright framework applicable to creator content — specifically, the provisions of the Copyright Act, 1957 governing fair dealing, user-generated content exceptions, and digital rights management — is relevant to creators who use third-party material (music, video clips) in their content and to platforms that implement content ID systems to manage copyright compliance. And the consumer protection and data protection frameworks applicable to creator platforms — particularly the obligations of significant social media intermediaries under the IT (Intermediary Guidelines) Rules — affect the conditions under which creators can access and monetise their audience data.

C.2 Fintech and Telecom Integration

The integration of telecommunications services and financial services — through mobile money (UPI, mobile wallets), telecom billing-based micropayment systems, and fintech applications delivered through telecom operator channels — is one of the most commercially and socially significant dimensions of India's digital economy. Mobile money, particularly UPI (Unified Payments Interface) — which processes billions of transactions monthly and has made India the

world's largest real-time payments market — is built on the telecommunications infrastructure of mobile broadband connectivity and uses the mobile subscriber's verified phone number as the primary identifier for payment initiation. The regulatory interface between telecommunications regulation (governing mobile connectivity and subscriber verification) and financial regulation (governing payment services and fintech products) is a critical governance consideration for this integrated ecosystem.

The RBI's regulatory jurisdiction over payment services — including UPI, mobile wallets, and payment aggregators — is distinct from TRAI's jurisdiction over telecommunications services, but the two regulatory regimes interact in important ways for entities that operate at the intersection. Telecom operators that offer payment services (as Jio does through Jio Pay, and as Airtel did through Airtel Payments Bank) are simultaneously subject to TRAI/DoT telecoms regulation (for their connectivity and mobile services) and RBI regulation (for their payment services). The data protection framework applicable to payment data (which RBI treats as highly sensitive) intersects with the DPDPA's general personal data protection framework, creating a complex multi-layered compliance environment for telecom operators with payment service offerings.

The intersection of cybersecurity obligations in the telecom and fintech context creates specific compliance challenges. A cyber attack that compromises a telecom operator's core network may also compromise payment services built on that network — for example, by enabling SIM swap attacks (fraudulently porting a subscriber's number to a new SIM under the attacker's control, enabling takeover of payment accounts linked to the phone number) or OTP interception (intercepting the one-time passwords sent by SMS for payment authentication). Telecom operators' responsibility for preventing SIM swap fraud — through robust subscriber verification requirements for port requests, rapid response to subscriber-reported fraudulent porting, and industry-level fraud monitoring systems — is both a direct customer protection obligation and a critical contribution to the security of the fintech ecosystem. The development of industry-wide SIM swap fraud prevention standards — coordinated between DoT, TRAI, RBI, and the telecom operators' industry association — is an important cybersecurity governance priority.

C.3 Smart Cities and Urban Telecom Infrastructure

Smart cities — urban environments equipped with ICT infrastructure enabling real-time monitoring, management, and optimisation of city services including traffic, energy, water, waste, public safety, and citizen services — represent one of the most commercially significant applications of telecommunications technology in the 5G era. India's Smart Cities Mission —

launched in 2015 with a target of developing 100 smart cities — has invested in ICT infrastructure across participating cities, including: integrated command and control centres (ICCCs) that aggregate data from across city systems; smart traffic management systems (using sensors, cameras, and dynamic signalling); smart water and energy metering; public Wi-Fi networks; and urban mobility platforms (integrating metro, bus, and shared mobility services). The telecommunications infrastructure underlying smart city deployments — including the IoT connectivity, edge computing, fibre backhaul, and data centre facilities — is a major and growing component of telecom operators' revenue opportunity in the urban enterprise segment.

The regulatory framework for smart city telecommunications involves multiple layers: the telecom regulatory framework (governing the connectivity services provided by licensed operators to smart city authorities and smart city application operators); the public procurement framework (governing how smart city authorities procure ICT services and infrastructure through competitive tendering); the data governance framework (governing how smart city systems collect, process, and use citizen data, including location data, behavioural data, and biometric data from public cameras); and the cybersecurity framework (governing the security of smart city ICT infrastructure, which typically includes systems controlling physical infrastructure like traffic signals and utility networks). The convergence of these regulatory dimensions in a single smart city deployment — where a telecom operator may simultaneously be a connectivity provider (subject to telecom regulation), a data processor (subject to DPDPA obligations), and a managed service provider for critical infrastructure (subject to security and resilience standards) — creates complex regulatory compliance obligations that require integrated management.

C.4 Digital Media and Content Regulation

The regulation of digital media content — online news, entertainment, user-generated content, and streaming media — intersects with the telecommunications regulatory framework in several important ways. Telecom operators that provide IPTV services (delivering linear television channels and video-on-demand content over their broadband networks) may be required to comply with content standards applicable to broadcasting (under the Cable Television Networks Regulation Act and the proposed Broadcasting Services Regulation Bill) in addition to the quality of service and consumer protection obligations of the telecom regulatory framework. Operators that carry Over-the-Top video content on their networks — as neutral bit-pipe providers — have generally been treated as passive intermediaries with no content liability; but if operators take active steps to filter or prioritise specific content (whether under legal obligation or for commercial reasons), their intermediary liability protection may be affected.

The proposed Broadcasting Services (Regulation) Bill — which seeks to bring OTT content platforms (Netflix, Amazon Prime, Hotstar, YouTube) within a broadcasting regulatory framework, subjecting them to content standards, certification requirements, and regulatory oversight — has significant implications for the relationship between telecom operators and OTT platforms. If OTT platforms are treated as broadcasters under the Bill, the "must carry" obligations that apply to broadcasting distribution platforms may extend to the internet access services of telecom operators — potentially requiring operators to ensure that all licensed OTT broadcasting services are accessible on their networks without blocking or throttling. The definition of "internet access" and its relationship to "distribution platform" under the proposed Bill is a key legal question that will determine the extent to which telecom operators are drawn into the regulatory framework for online broadcasting.

C.5 Telecommunications and Electoral Law

The intersection of telecommunications and electoral law — governing the use of telecommunications services for political communication, voter outreach, electoral campaigning, and electoral administration — is a significant dimension of India's democratic governance framework with specific implications for telecom operators. The Election Commission of India's Model Code of Conduct (MCC) — which restricts the use of government resources for political campaigning during election periods — has been applied in the context of telecommunications to address the use of government-controlled telecom infrastructure (including BSNL and MTNL networks) for political communication. The DoT and TRAI are required to ensure that their regulatory decisions during election periods do not favour or disadvantage specific political parties — an obligation that creates a degree of regulatory restraint during electoral seasons that practitioners advising on regulatory timelines must factor into their advice.

The Do Not Disturb (DND) registry and the Unsolicited Commercial Communication (UCC) regulation framework have direct relevance to electoral communication. Political parties and electoral campaigns are significant users of bulk SMS and robocall services — the same services regulated under the UCC framework — to reach voters during election campaigns. The question of whether political communication (by registered political parties, candidates, and their authorised agents) should be exempted from the DND registry requirements that apply to commercial communication — or whether voters should be protected from unsolicited political calls and messages in the same way they are protected from commercial solicitation — is a policy question that TRAI has addressed in its successive DND and UCC regulatory consultations. The current framework provides limited exemption for political communication during defined election periods, reflecting a balance between political parties' legitimate interest

in communicating with voters and voters' interest in controlling the communications they receive on their personal telecommunications devices.

C.6 The Legal Framework for Open Data in Telecom

Open data initiatives in the telecommunications sector — the structured sharing of non-commercially sensitive, aggregated telecommunications data with researchers, policymakers, and the public — can generate significant social and economic benefits while maintaining appropriate protection for commercially sensitive and personally identifiable information. TRAI's publication of quarterly Quality of Service performance reports, its publication of telecom subscription data, and its publication of internet speed measurement data through the MySpeed portal are examples of existing open data initiatives in the Indian telecom regulatory space. The development of a more comprehensive open data framework — potentially including anonymised aggregate network performance data (traffic volumes by geography and time), spectrum utilisation data, and coverage measurement data — would enable researchers, local authorities, and businesses to make better-informed decisions about connectivity infrastructure investment, location planning, and digital service deployment.

The legal framework for open data in the telecom sector must address several tensions: commercial sensitivity (operators may resist sharing data that reveals commercially valuable information about their network performance, subscriber density, or market share); personal data protection (aggregate data must be adequately anonymised to prevent re-identification of individuals, consistent with DPDPA requirements for data minimisation and purpose limitation); national security (some categories of network data, particularly data about network topology and capacity in sensitive areas, may be sensitive for national security reasons); and intellectual property (operators may claim intellectual property rights in their network data, though the legal basis for such claims is uncertain). A carefully designed open data framework — specifying the categories of data to be shared, the aggregation and anonymisation standards required, the publication mechanism, and the permitted uses of published data — could capture the public benefits of open telecom data while adequately protecting the legitimate interests of operators and subscribers.

SUPPLEMENTARY NOTE D

Digital Economy and Emerging Law

D.1 Online Dispute Resolution for Telecom Consumers

Online dispute resolution (ODR) — the use of digital platforms and communication technologies to resolve disputes without physical attendance at a tribunal or court — has emerged as an important complement to traditional legal processes for resolving high-volume, low-value consumer disputes of the kind that arise in the telecommunications sector. The development of telecom-specific ODR mechanisms — enabling subscribers to resolve billing disputes, service quality complaints, and contractual disagreements with operators through online platforms, with or without the involvement of a neutral third party — has the potential to significantly improve consumer access to justice in the telecommunications sector. Traditional dispute resolution mechanisms (consumer courts, CGRF forums, TDSAT) are appropriate for significant disputes but are disproportionate for the small-value, high-frequency disputes that characterise most telecom consumer grievances. An effective ODR mechanism — combining automated resolution algorithms (for straightforward billing disputes where the facts can be verified against the operator's records), online mediation (for disputes requiring negotiation between the subscriber and the operator), and online arbitration (for disputes that cannot be resolved through negotiation but do not warrant formal tribunal proceedings) — would provide proportionate, affordable, and rapid resolution for the vast majority of telecom consumer disputes.

The legal framework for telecom ODR in India is currently underdeveloped. The Consumer Protection Act, 2019 contemplates the use of mediation for consumer disputes and enables the Central Government to develop ODR frameworks for consumer disputes generally. The Telecommunications Act, 2023 does not specifically provide for ODR, but the general ADR provisions and the framework for consumer protection under the authorisation conditions provide a basis for developing telecom-specific ODR mechanisms. TRAI's engagement with ODR — through its consultation on consumer protection and the development of a technology-enabled grievance management platform — has been primarily focused on improving the first-tier complaint resolution process (the operator's customer care function) rather than developing a true ODR mechanism with neutral third-party involvement. The development of an industry-funded, TRAI-supervised ODR platform for telecom consumer disputes — modelled on successful ODR implementations in other sectors (such as the RBI's Ombudsman scheme for banking and the IRDAI's Bima Bharosa scheme for insurance) — would significantly improve the consumer protection landscape for telecommunications subscribers while reducing the burden on TDSAT of individual consumer matters.

The application of AI and natural language processing to telecom dispute resolution — enabling automated analysis of complaint descriptions, matching of complaints against standard

resolution patterns, and automated generation of resolution proposals based on the operator's obligations and the subscriber's rights — is an emerging frontier in regulatory technology that could transform the efficiency of consumer dispute resolution. An AI-assisted ODR system for telecom disputes could: automatically categorise complaints by type and route them to the appropriate resolution pathway; verify factual claims (such as claims about call drop rates, billing amounts, or service coverage) against the operator's network records; apply the applicable regulatory standards (TRAI's QoS benchmarks, the licence fee conditions, the billing regulations) to generate a regulatory assessment of the complaint; and propose a resolution that complies with the regulatory framework. The legal and ethical implications of AI-assisted dispute resolution — including the accountability for AI-generated resolution proposals, the right of parties to human review of AI determinations, and the data protection implications of sharing subscriber data with an AI dispute resolution system — require careful regulatory design before such systems can be deployed at scale.

D.2 The Legal Treatment of Network Slices in 5G

The network slicing capability of 5G — enabling operators to create multiple virtual network instances on a single physical 5G infrastructure, each with distinct quality-of-service characteristics optimised for different use cases — creates novel legal and regulatory questions about the classification and treatment of network slices that India's telecommunications regulatory framework must address. From a technical perspective, a network slice is a logical partition of the 5G network resources (spectrum, computing, and transmission capacity) configured to provide defined quality characteristics for a specific use case. From a regulatory perspective, the question is whether a network slice constitutes a distinct telecommunications service (requiring its own regulatory assessment and potentially its own authorisation) or whether it is simply a quality-differentiated form of the same connectivity service already authorised under the operator's access service authorisation. The answer has significant implications for: the licensing framework (whether separate authorisations are needed for specific types of network slice); the net neutrality framework (whether providing differentiated quality to users of specific network slices violates the non-discrimination principle); and the consumer protection framework (what quality guarantees must an operator provide to a subscriber purchasing connectivity delivered through a specific network slice).

TRAI's 2017 recommendations on net neutrality — which addressed network slicing as an emerging technology at that time — distinguished between "specialised services" (network slices provided for specific managed service use cases, distinct from internet access) and "internet access services" (connectivity to the public internet, subject to net neutrality requirements). This

distinction provides a framework for addressing the net neutrality dimensions of network slicing, but does not resolve all the regulatory questions raised by 5G network slice-based services. Specifically: how should a network slice that provides internet access at guaranteed quality to enterprise users (rather than best-effort quality to retail users) be classified? Is it a "specialised service" (because it has specific quality guarantees) or an "internet access service" (because it provides access to the internet)? And if an operator provides guaranteed-quality internet access to enterprise users through a network slice while providing best-effort internet access to retail users, does this constitute a violation of the net neutrality principle (because the enterprise users have better access to internet services than retail users) or a legitimate quality-differentiated commercial offering (because the enterprise users are paying for a higher tier of service)?

The development of a clear regulatory framework for 5G network slice-based services — addressing the licensing, net neutrality, consumer protection, and interconnection questions — is an important priority for TRAI and DoT as 5G commercial deployments accelerate. The framework should distinguish clearly between: (a) network slices providing managed enterprise services (such as private network connectivity for a factory campus, V2X connectivity for a smart highway, or critical communications for a hospital network) that are genuinely distinct from internet access and do not raise net neutrality concerns; (b) network slices providing premium quality-of-service internet access to enterprise or consumer subscribers (which may raise net neutrality concerns if the premium quality is unavailable to all subscribers at similar prices); and (c) network slices providing internet access to specific content providers' traffic (for example, a Netflix slice providing high-quality streaming) which directly raises net neutrality concerns if other content providers cannot access equivalent quality treatment on equivalent commercial terms.

D.3 Regulatory Framework for Space-Based Services

The regulatory framework for space-based telecommunications services in India — encompassing both traditional geostationary satellite services (VSAT, satellite broadband, satellite broadcasting) and emerging non-geostationary orbit (NGSO) services from LEO constellations — is evolving rapidly in response to both technological developments (the LEO broadband revolution) and policy changes (India's new space policy and IN-SPACe's mandate). The legal framework involves multiple regulatory dimensions: the space segment regulation (IN-SPACe authorisation for satellite operations, including launch and on-orbit operations); the telecommunications services regulation (DoT authorisation for providing communication services using satellite infrastructure); the spectrum regulation (WPC frequency assignments for earth station uplink and downlink frequencies); and the consumer protection regulation (TRAI's QoS and consumer protection standards applicable to satellite communication services). The

coordination between these regulatory dimensions — historically managed through informal inter-agency consultation — is being formalised through the evolving space regulatory framework and the Telecommunications Act, 2023's implementing rules.

The entry of foreign LEO satellite broadband providers into the Indian market — specifically the Starlink (SpaceX), OneWeb/Eutelsat, and Amazon Kuiper platforms — requires a regulatory framework that balances India's interest in accessing best-in-class global satellite technology with the need to protect national security, ensure consumer protection, and maintain regulatory oversight of services provided to Indian subscribers by foreign-operated infrastructure. The security conditions applicable to foreign-operated satellite broadband services — specifically the requirements for lawful interception capability, subscriber data localisation, and compliance with directions from Indian regulatory authorities — are particularly complex to implement for services delivered through satellites operated by foreign companies from data centres outside India. The development of a practical, technically feasible framework for regulatory compliance by foreign satellite broadband operators — one that achieves India's legitimate security and regulatory objectives without creating barriers that are so demanding as to deter market entry by best-in-class operators — is one of the most challenging regulatory design problems in India's evolving digital governance agenda.

D.4 Technology and the Rule of Law in Digital Governance

The rapid pace of technological change in the telecommunications and digital sectors creates a persistent challenge for the rule of law: legal frameworks that are calibrated to today's technology landscape become outdated quickly, creating gaps and ambiguities that parties exploit and that courts and regulators must resolve through creative interpretation or administrative guidance rather than clear legislative text. The Telecommunications Act, 2023's adoption of technology-neutral language — defining "telecommunication services" in terms of the function performed (enabling communication) rather than the technology used — is a deliberate legislative strategy for improving the law's durability in the face of technological change. Technology-neutral definitions allow the law to evolve with technology without requiring constant amendment, ensuring that new communication technologies (whether satellite broadband, quantum communications, or technologies not yet invented) are captured by the legal framework if they perform the function that the law seeks to regulate. However, technology-neutral language also creates definitional uncertainty — the question of whether a specific new technology falls within a broadly defined category requires case-by-case interpretation that may produce inconsistent results unless the regulator provides clear guidance through secondary legislation or administrative interpretation.

The "digital rights" dimension of telecommunications governance — the recognition that access to digital communications services is increasingly a precondition for the effective exercise of fundamental rights including freedom of expression, freedom of association, access to education, economic participation, and political participation — places telecommunications regulation squarely within the domain of constitutional rights. The Supreme Court's recognition in Anuradha Bhasin that the right to access the internet is a fundamental right under Article 19(1)(a) is the most direct expression of this constitutional dimension. But the digital rights framework extends beyond the specific right to internet access: the right to privacy (Puttaswamy) constrains telecommunications surveillance; the right to equal protection (Article 14) constrains discriminatory regulation of different user groups or operators; and the right to carry on a trade or profession (Article 19(1)(g)) constrains regulatory measures that unreasonably restrict operators' commercial freedom. Together, these constitutional constraints form a rights-based framework for telecommunications regulation that practitioners must understand and apply in advising on both the design of regulatory frameworks and the exercise of regulatory powers.

D.5 Post-2030 Outlook: Digital Infrastructure Law

The legal framework for India's digital infrastructure in the period beyond 2030 — when 6G technology will be approaching commercial deployment, AI will be deeply embedded in network operations, quantum communications will be transitioning from research to operational use, and the internet of everything will be connecting billions of devices — must be designed with long-term durability in mind. The Telecommunications Act, 2023 represents a significant improvement on the 1885-vintage Indian Telegraph Act it replaces, providing a more modern, flexible, and constitutionally grounded framework for telecommunications governance. But the 2023 Act's specific provisions will inevitably require updating as technology and market structures evolve. The key design principle for durable telecommunications legislation — drafting in terms of functions, outcomes, and principles rather than in terms of specific technologies, market structures, or regulatory tools — is imperfectly implemented in the 2023 Act, which necessarily reflects the specific technology and market context of 2023 in some of its detailed provisions. The development of secondary legislation under the 2023 Act — the rules, regulations, and authorisation conditions that give specific operational content to the Act's broad framework — is where the ongoing task of keeping India's telecommunications legal framework current with technological developments will primarily occur.

India's ambition to be a global leader in digital governance — exporting its DPI model, promoting a balanced approach to AI regulation, contributing to international standards for satellite communications and 6G, and advocating for developing-country perspectives in global

digital governance forums — requires that India's own domestic legal framework be internationally credible. A telecommunications regulatory framework that is seen as overly restrictive (inhibiting innovation and investment), insufficiently protective of privacy and freedom of expression (undermining digital rights), or institutionally fragile (subject to arbitrary executive interference) will undermine India's credibility as a proponent of good digital governance globally. Conversely, a framework that effectively balances connectivity (through universal service obligations and competitive market development), security (through proportionate surveillance and cybersecurity requirements), and rights (through constitutional constraints on government action) will strengthen India's standing as a model for the developing world. The Telecommunications Act, 2023 — and its implementation over the coming years — will be judged by this international standard as well as by domestic measures of consumer welfare and market development.

SUPPLEMENTARY NOTE E

Digital Future: Extended Analysis

E.1 Telecom Law and Climate Change

The intersection of telecommunications law and climate change law is emerging as an important regulatory frontier as India pursues its ambitious climate commitments (Net Zero by 2070, 500 GW of renewable energy capacity by 2030) while simultaneously expanding its telecommunications infrastructure. The telecommunications sector's contribution to climate change occurs through: energy consumption (mobile base stations, data centres, and network equipment collectively consume significant quantities of electricity, a substantial portion of which is generated from fossil fuels in India's current energy mix); equipment lifecycle emissions (the manufacturing, transportation, and end-of-life disposal of billions of connected devices generates lifecycle carbon emissions that must be counted in the sector's total climate impact); and infrastructure construction emissions (the construction of towers, data centres, and cable systems involves cement, steel, and other carbon-intensive materials). The telecommunications sector can also contribute to climate solutions: smart grid infrastructure (using 5G IoT connectivity to manage renewable energy integration), precision agriculture (using satellite and cellular connectivity to reduce resource waste in farming), and remote working (reducing transport emissions by enabling workers to work from home) are all applications of telecommunications technology that have significant climate benefits.

The regulatory framework for telecommunications and climate change in India is nascent but developing. TRAI's consultation on sustainable telecommunications (2021) addressed energy efficiency standards for network equipment and renewable energy mandates for telecom infrastructure, but did not establish binding regulatory requirements. The Bureau of Energy Efficiency's (BEE) energy efficiency standards for electrical equipment may be extended to include telecommunications network equipment, requiring base stations, data centres, and routers to meet minimum energy efficiency standards. The Environment Ministry's Extended Producer Responsibility (EPR) framework for electronic waste — requiring telecom equipment manufacturers and operators to ensure the responsible recycling of end-of-life equipment — creates specific compliance obligations for operators managing large fleets of network equipment and subscriber devices. The Telecommunications Act, 2023's framework does not explicitly address climate change or environmental sustainability, but the Central Government's power to prescribe conditions of authorisation provides the legislative basis for including environmental sustainability conditions in authorisations — a regulatory option that DoT and TRAI may exercise as India's climate commitments intensify.

The specific climate-related challenges for telecommunications infrastructure in India include the increasing frequency and intensity of extreme weather events (cyclones, floods, and heat waves) that damage telecommunications infrastructure and disrupt services. India's vulnerability to climate-related infrastructure disruption — with major cyclones regularly affecting coastal telecommunications infrastructure and with flooding periodically disrupting ground-level infrastructure in river plains — is a growing operational and regulatory challenge. The climate resilience dimension of telecommunications infrastructure — designing infrastructure to withstand more severe weather events, installing backup power systems that function during extended grid outages caused by extreme weather, and maintaining rapid disaster recovery capabilities for post-event network restoration — is increasingly relevant for the critical infrastructure protection framework under the Telecommunications Act, 2023. The integration of climate resilience requirements into the authorisation conditions and the critical infrastructure protection framework — requiring operators to assess and address the climate-related risks to their infrastructure and to develop climate adaptation plans — is an important regulatory agenda item that DoT and TRAI should address proactively.

E.2 Health Technology and Telecommunications

The rapidly growing digital health sector in India — encompassing telemedicine, remote patient monitoring, digital health records, AI-assisted diagnostics, and health data analytics — is one of the most socially significant applications of telecommunications connectivity and digital

infrastructure. The National Digital Health Mission (NDHM) — now operating as Ayushman Bharat Digital Mission (ABDM) — provides the foundational digital infrastructure (Health IDs, Health Facility Registry, Health Professional Registry, and Health Data Exchange) that enables the digital health ecosystem. Telecommunications connectivity is the enabling layer for ABDM: patients in remote areas can access telemedicine services only if they have adequate broadband connectivity; remote patient monitoring devices require reliable IoT connectivity to transmit health data; and the ABDM's health data exchange requires secure, high-availability connectivity between health facilities, health data repositories, and health technology applications. The regulatory interface between telecommunications regulation (governing the connectivity services) and digital health regulation (governing the health applications and data) creates specific compliance considerations for companies providing telecoms-enabled health services.

The telemedicine regulatory framework in India — governed by the Telemedicine Practice Guidelines issued by the Medical Council of India (now the National Medical Commission) in 2020 — places specific requirements on the telecommunications services used for telemedicine consultations: the consultation must be conducted through a secure, authenticated communication channel; the platform must comply with the IT Act's security and privacy requirements; and the communication must be of sufficient quality to enable a meaningful clinical assessment. Telecommunications operators and OTT communication service providers that offer telemedicine-specific communication services — designed to meet the clinical quality and security requirements of medical consultations — occupy a distinct regulatory space that combines telecommunications regulation with digital health regulation. The development of a specific quality of service standard for telemedicine communications — covering video resolution, audio clarity, latency, security, and authentication — within TRAI's QoS regulatory framework would provide clarity for operators and platforms providing telemedicine communication services and ensure that the telecommunications layer of telemedicine meets the clinical quality requirements of medical practice.

E.3 Legal Dimensions of the Space Economy

The commercial space economy — encompassing satellite launches, satellite operations, space tourism, asteroid mining, and in-space manufacturing — is entering a phase of rapid growth that creates novel legal questions at the intersection of national telecommunications law, international space law, and commercial contract law. India's commercial space sector is developing rapidly, with IN-SPACe's authorisation framework enabling private sector space activities and the New Space Policy, 2023 providing the strategic direction. Several Indian companies — including Skyroot Aerospace (which completed India's first privately developed

rocket launch in 2022), Agnikul Cosmos, and Bellatrix Aerospace — are developing launch vehicles and satellite technologies that will enable a domestic commercial space launch capability. The telecommunications applications of this emerging space capability — particularly the development of domestic satellite broadband constellations and the provision of satellite-based connectivity services using domestically developed and launched satellites — are directly relevant to India's telecommunications regulatory framework.

The legal framework for satellite operations under India's space regulatory regime involves: IN-SPACe authorisation for the space activities (launch, on-orbit operations, and de-orbit); DoT authorisation for the telecommunications services provided using the satellite; and ITU coordination for the frequency assignments associated with the satellite. The liability framework for damage caused by Indian satellites — governed by the Space Liability Convention (1972), to which India is a party — provides that India is liable internationally for damage caused by space objects launched from Indian territory or by Indian nationals. This international liability creates a regulatory rationale for India to maintain oversight of all Indian space activities through IN-SPACe authorisation, ensuring that only responsible, safety-compliant operators are permitted to launch satellites that could create international liability exposure. The development of domestic space insurance requirements — requiring satellite operators to maintain insurance against third-party liability claims arising from satellite operations — would both implement India's international liability obligations and create a market-based mechanism for ensuring that Indian space operators maintain safety standards adequate to manage their liability exposure.

The emerging concept of "space traffic management" — the governance framework for coordinating the movements and communications of the growing population of satellites, space stations, and other objects in Earth orbit — is one of the most important long-term governance challenges for the global space community and has direct implications for India's telecommunications regulatory framework. As India develops its commercial space sector and increases the number of Indian satellites in orbit, India's stake in the development of an effective international space traffic management framework grows correspondingly. The legal basis for space traffic management — currently rudimentary, based primarily on the voluntary guidelines of the Inter-Agency Space Debris Coordination Committee and the ITU's satellite coordination procedures — will need to be substantially strengthened through new international agreements if the growing space object population is to be managed safely. India's active engagement in the development of international space traffic management norms — through the UN Committee on the Peaceful Uses of Outer Space (COPUOS), the ITU, and bilateral space cooperation arrangements — is both a national interest priority and a global public good contribution that

reflects India's growing role as a responsible space power.

SUPPLEMENTARY NOTE F

Digital Economy: Closing Analysis

F.1 Cross-Platform Data Portability in Telecom

Data portability — the right of individuals to receive their personal data in a structured, commonly used, and machine-readable format and to transfer it to another service provider — is a consumer right with specific relevance in the telecommunications context. Telecommunications subscribers accumulate significant personal data with their operators over the course of their subscription: call records, data usage records, location history, device configuration, service preferences, and account data. Under the DPDPA, 2023, subscribers have the right to request this data in a portable format. The practical implementation of data portability for telecommunications subscribers — what specific data categories must be included in a portability request, in what format the data must be provided, within what timeline, and through what mechanism — requires regulatory guidance that TRAI and the Data Protection Board have not yet fully provided. The technical standards for telecommunications data portability — building on international standards such as the W3C's Portable Contacts specification and the data portability frameworks being developed in the EU context — should be developed through a coordinated process involving TRAI, the Data Protection Board, and the telecommunications industry.

The competitive implications of telecommunications data portability are significant and potentially transformative. If subscribers can easily transfer their complete telecommunications data history (including call records, usage patterns, and service preferences) to a new operator when switching, the data advantage currently enjoyed by long-established operators (who have extensive histories of subscriber behaviour) will be diminished. This could intensify competition: new operators or new entrants would have access to the same quality of subscriber data as incumbents (because subscribers can transfer their historical data), removing a competitive advantage that currently tends to entrench existing operator-subscriber relationships. Conversely, operators may resist data portability requirements precisely because they undermine the competitive advantage of accumulated subscriber data. TRAI's regulatory approach to telecommunications data portability should assess both the consumer welfare benefits of portability (enabling effective switching, reducing lock-in effects) and the competitive dynamics implications (improving new entry prospects, reducing barriers to subscriber

switching).

The interoperability dimension of telecommunications data portability — specifically whether telecommunications operators can be required to make their subscriber data management systems interoperable with other operators' systems, enabling automatic data transfer when a subscriber switches — is a more ambitious form of portability that goes beyond providing a data export to the switching subscriber. Interoperability-based portability would create a technical infrastructure for seamless data transfer between operators when subscribers switch, potentially without the subscriber needing to actively manage the transfer process. The regulatory framework for such interoperability — requiring operators to implement standardised data exchange APIs and to participate in a coordinated data transfer mechanism — would be a significant technical and commercial mandate that requires careful stakeholder consultation and technical standardisation work before it can be practically implemented. The development of a phased approach to telecommunications data portability — starting with basic data export rights and progressively moving toward technical interoperability — would enable early consumer benefits from portability while allowing time for the technical and governance frameworks needed for full interoperability to be developed.

F.2 Autonomous Telecom Networks and Governance

The concept of autonomous telecommunications networks — networks that use artificial intelligence and machine learning to manage themselves with minimal human intervention, dynamically optimising spectrum allocation, traffic routing, security responses, and energy consumption in real-time — represents the long-term vision for 6G and beyond-6G telecommunications technology. Autonomous network management builds on the closed-loop automation already deployed in advanced 4G/5G networks (where algorithms automatically adjust base station parameters to optimise coverage and capacity) toward a fully autonomous system where the network learns, adapts, and self-heals without human direction. The performance benefits of autonomous network management are significant: AI-driven networks can respond to changing traffic patterns, security threats, and equipment failures faster and more accurately than human network operations teams, potentially delivering better quality of service with lower operational costs. The regulatory challenges of autonomous network management are, however, equally significant: when an autonomous algorithm makes a network management decision that affects millions of subscribers (for example, a decision to redirect traffic in a way that creates congestion in one area to relieve congestion in another), who is accountable for that decision?

The accountability framework for autonomous telecommunications network management must address several distinct governance questions. First, the transparency question: can the network operator explain, in human-understandable terms, why the autonomous management system made a specific decision? The "explainability" requirement — increasingly recognised as essential for AI systems that make consequential decisions — is particularly challenging for deep learning AI systems, where the decision logic is distributed across millions of parameters in a neural network that cannot be straightforwardly interpreted by humans. Second, the audit question: can the autonomous management system's decisions be retrospectively reviewed, to assess whether they complied with regulatory requirements (net neutrality, quality of service, non-discrimination) and to identify any systematic biases or errors? Third, the liability question: when an autonomous network management decision causes harm to a subscriber (for example, a misrouted emergency call or a security response that blocks a legitimate communication), who bears responsibility — the operator that deployed the autonomous system, the AI developer that designed the algorithm, or neither? The development of regulatory standards for explainability, audit trails, and liability in autonomous network management — informed by the general AI governance frameworks being developed by MEITY and aligned with the EU AI Act's high-risk AI provisions — is an important regulatory priority for the 6G era.

The security implications of autonomous telecommunications network management create specific concerns that the regulatory framework must address. An autonomous network management system that can dynamically reconfigure network parameters, update software, and respond to security threats is also a potential attack vector: an attacker who can compromise the autonomous management system can use it to cause widespread network disruption, redirect traffic for eavesdropping, or disable security protections at scale. The security architecture for autonomous network management systems — including the authentication and integrity protection of the AI model and its inputs, the isolation of the management system from the operational network, and the human override mechanisms that can disable the autonomous system in the event of unexpected behaviour — must be designed to the highest security standards. The Trusted Telecom Portal framework, as it evolves to address 6G and autonomous network technology, must incorporate specific evaluation criteria for autonomous network management systems, assessing their security architecture, adversarial robustness (resistance to attacks specifically designed to mislead the AI), and the adequacy of their human oversight mechanisms.

F.3 Regulatory Technology Innovation

Regulatory technology (RegTech) — the application of technology to improve the efficiency, accuracy, and compliance of regulatory processes — is transforming the practice of telecommunications regulation in ways that have significant legal and institutional implications. RegTech applications relevant to telecommunications regulation include: automated compliance monitoring (using AI to analyse operators' reported data and identify potential compliance issues without manual review); real-time spectrum monitoring (using software-defined radio technology to detect unauthorised spectrum use and interference without relying on complaint-based detection); digital regulatory reporting (using standardised application programming interfaces to collect regulatory data directly from operators' operational systems, reducing manual reporting burden and improving data accuracy); and AI-assisted regulatory analysis (using natural language processing and machine learning to analyse large volumes of public submissions to consultations, identify key themes and arguments, and assist regulatory staff in preparing response analyses).

The legal framework for RegTech applications in Indian telecommunications regulation — specifically the questions of what data TRAI and DoT may collect from operators through digital means, how that data may be used, and what procedural protections operators have against regulatory decisions based solely on automated data analysis — is still developing. The general legal authority for TRAI's information collection (under Section 12 of the TRAI Act) and DoT's licence condition reporting requirements provide the existing legal basis for digital regulatory reporting. However, the specific legal standards applicable to automated compliance monitoring — where a regulatory algorithm rather than a human reviewer identifies potential violations — raise specific procedural fairness questions: should operators be notified when an automated system flags their data as potentially non-compliant? What human review must occur before a compliance finding based on automated analysis is acted on? And what opportunities must operators have to contest automated compliance determinations before enforcement action is initiated? The development of published guidelines on TRAI's and DoT's RegTech practices — clarifying the role of automated systems in compliance monitoring and the human review requirements before enforcement action — would improve the procedural fairness of automated compliance monitoring and provide operators with clearer expectations about the standards to which their reported data will be held.

F.4 Competition and Innovation in the 5G Ecosystem

The 5G ecosystem — the broader commercial landscape of hardware manufacturers, software developers, systems integrators, and application developers that participate in the value chain of 5G services — presents specific competition and innovation policy challenges that

require regulatory attention beyond the traditional mobile operator-centric focus of telecommunications regulation. The 5G value chain is more complex and diverse than previous generations: where 4G was primarily a mobile broadband technology with a relatively straightforward value chain (device manufacturers, network equipment vendors, operators, and subscribers), 5G enables applications across dozens of vertical industries (manufacturing, healthcare, transportation, energy, agriculture) with complex multi-party value chains involving sector-specific technology providers, systems integrators, and enterprise customers alongside the traditional telecommunications actors. The competition dynamics of this more complex value chain — and specifically the potential for market power concentration at specific points (such as in network equipment, AI-driven network management software, or specific vertical industry platforms) — create competition law challenges that India's regulatory framework must address.

The standard essential patent (SEP) licensing framework — which governs access to the fundamental technology patents that must be licensed to implement 5G standards — is one of the most commercially contentious aspects of the 5G ecosystem from a competition law perspective. 5G technology is built on patented inventions contributed by hundreds of companies to the 3GPP standardisation process; any company that manufactures or operates 5G equipment must license these standard essential patents. The SEP holders (primarily Ericsson, Nokia, Qualcomm, Huawei, Samsung, and other major technology companies) are required to license their SEPs on "fair, reasonable, and non-discriminatory" (FRAND) terms under the IP policies of the relevant standards bodies. In practice, the determination of what royalty rate constitutes a FRAND royalty has been the subject of major patent litigation globally, with Indian courts (particularly the Delhi High Court) having heard some of the most significant FRAND licensing disputes, including proceedings involving Ericsson and smartphone manufacturers. TRAI and CCI's engagement with the SEP licensing framework — through regulatory monitoring of SEP licensing practices and competition law enforcement against abusive SEP licensing — is important for ensuring that the FRAND framework works as intended and does not create barriers to 5G equipment manufacturing in India.

SUPPLEMENTARY NOTE G

Digital Economy Law: Final Analysis

G.1 The Legal Framework for Content Delivery Networks

Content Delivery Networks (CDNs) — distributed networks of servers that cache and deliver internet content from locations close to the end user, reducing latency and improving delivery

speed — are critical infrastructure for the modern internet, carrying a large proportion of global internet traffic including streaming video, software downloads, and web content. India's CDN ecosystem has developed significantly over the past decade, with major global CDN providers (Akamai, Cloudflare, Amazon CloudFront, and Google) establishing Points of Presence (PoPs) in India's major cities, and Indian operators and infrastructure providers developing domestic CDN capabilities. The regulatory framework for CDNs in India occupies an uncertain position: CDN providers are not telecommunications operators (since they do not transmit signals between points as licensed telecoms operators do) and are not ISPs (since they do not provide internet access to end users), but their network infrastructure and their commercial relationships with ISPs (through peering and transit arrangements at internet exchange points) have significant implications for the quality of internet service delivered to Indian subscribers.

The net neutrality dimensions of CDN arrangements raise specific regulatory questions about the relationship between ISPs' commercial arrangements with CDN providers and the non-discrimination principle applicable to internet access services. An ISP that gives preferential treatment to traffic from a specific CDN provider — through lower prices for CDN peering, priority routing for CDN traffic, or inclusion of CDN traffic in "zero-rated" data allowances — may be providing an advantage to the CDN provider (and by extension to the content companies that use that CDN) over competitors that use other CDNs or that deliver content directly without CDN intermediation. TRAI's net neutrality framework — which prohibits differential treatment of content based on its source, destination, or type — applies directly to ISPs' treatment of CDN traffic: an ISP cannot prefer traffic from one CDN over another, or prefer CDN-delivered traffic over directly-served traffic, without violating the non-discrimination principle. The enforcement of this principle in the context of CDN arrangements — which are commercially complex and technically difficult to monitor — requires TRAI to develop specific guidance on what CDN-related ISP conduct constitutes impermissible discrimination.

The data privacy implications of CDN arrangements — specifically the processing of subscriber request data by CDN providers that serve content to Indian subscribers — require analysis under the DPDPA's data processing framework. When an Indian subscriber requests content that is served through a CDN, the CDN provider processes the subscriber's IP address (to determine the appropriate server to use), the content requested (to select the appropriate cached response), and potentially other request metadata. This processing constitutes the processing of personal data (since the subscriber's IP address can be used to identify them, at least approximately) by a data processor (the CDN provider) on behalf of a data fiduciary (the content provider or the ISP). The DPDPA's requirements for data processing agreements

between data fiduciaries and data processors — ensuring that CDN providers process subscriber data only for the specified purpose, maintain appropriate security, and comply with Indian data protection requirements — create specific compliance obligations for the CDN ecosystem. The development of standard data processing agreement templates for CDN arrangements — covering the specific data flows and processing purposes of CDN operations — would reduce compliance transaction costs for both CDN providers and the content companies and ISPs that use CDN services.

G.2 Regulatory Framework for Cloud-Native Telecom

The cloudification of telecommunications — the migration of telecommunications network functions from dedicated hardware appliances to virtualised software running on commercial cloud infrastructure (whether private cloud operated by the operator, public cloud operated by hyperscalers such as AWS, Azure, or Google Cloud, or hybrid cloud combining both) — is one of the most significant infrastructure transformations in the telecommunications sector and creates important regulatory challenges that India's framework must address. Cloud-native telecommunications infrastructure offers significant benefits: reduced capital costs (from sharing infrastructure with other cloud users), operational flexibility (from the ability to dynamically scale capacity), faster deployment of new network functions (from the software-defined architecture), and improved resilience (from the geographic distribution and redundancy built into cloud infrastructure). However, cloud-native telecommunications also raises specific regulatory concerns: the location of network data and functions on third-party cloud infrastructure raises data sovereignty and security concerns; the dependence on hyperscaler cloud platforms creates concentration risk (if the hyperscaler experiences an outage, the operator's entire cloud-native network is affected); and the complex multi-vendor, multi-cloud architecture of cloud-native networks makes security auditing and regulatory compliance assessment more difficult than for traditional dedicated hardware deployments.

The Trusted Telecom Portal framework's application to cloud-native telecommunications poses specific technical challenges. Traditional TTP evaluation assesses hardware appliances — the physical boxes that perform specific network functions — against security standards. In a cloud-native architecture, the network function is a software container running on generic cloud compute infrastructure; there is no dedicated hardware to evaluate, and the security of the network function depends on both the software itself and the security of the underlying cloud infrastructure. The TTP framework must evolve to address cloud-native deployments by: developing evaluation criteria specifically for software-defined network functions (assessing code security, container security, and the security of interfaces to other network functions); requiring

security assessment of the cloud infrastructure on which licensed network functions run (either through a separate TTP evaluation of the cloud platform or through the acceptance of existing cloud security certifications such as ISO 27017 and SOC 2 Type II); and developing guidelines for the security management of multi-vendor cloud-native deployments (addressing the specific risks that arise from the interaction between network function software from multiple vendors running on shared cloud infrastructure).

The regulatory jurisdiction implications of cloud-native telecommunications — where critical network functions run on infrastructure owned and operated by global hyperscaler companies in data centres that may be located outside India — create specific data sovereignty and regulatory access concerns. When the core network function of an Indian telecommunications operator runs on infrastructure operated by a US hyperscaler in data centres located in Singapore or the United States, Indian regulatory authorities face practical difficulties in exercising their oversight and enforcement jurisdiction: they cannot physically access the data centres, they cannot directly inspect the network function software, and they cannot easily compel the hyperscaler to provide access to data or records stored in foreign data centres. The resolution of these jurisdictional challenges requires both contractual provisions (operators must ensure that their cloud service agreements give them — and by extension Indian regulatory authorities — the rights and access needed for compliance and oversight) and regulatory guidance (specifying what Indian regulatory authorities may require of operators using foreign cloud infrastructure and what operators must contractually secure from their cloud providers to fulfil these requirements). The development of specific cloud governance requirements for licensed telecommunications operators — addressing data localisation, audit access, disaster recovery, and regulatory notification requirements for cloud-native deployments — is an important regulatory priority under the Telecommunications Act, 2023's security framework.

G.3 Digital Twins in Urban Infrastructure

The deployment of digital twin technology for urban telecommunications infrastructure management — creating virtual models of city-wide telecommunications networks that enable real-time monitoring, predictive maintenance, and capacity planning — represents an important application of advanced ICT at the intersection of telecommunications, urban management, and data governance. A city-wide telecommunications digital twin integrates: real-time network performance data (from operators' network management systems); physical infrastructure data (tower locations, fibre routes, equipment specifications); usage patterns (anonymised traffic density data by geographic area and time); and external data sources (weather, events, construction activities that affect network performance). This integrated data model enables city

authorities and telecommunications operators to: identify coverage gaps and plan infrastructure improvements; anticipate network capacity requirements for large events or emergencies; coordinate infrastructure maintenance to minimise disruption; and optimise spectrum usage across the city's telecommunications infrastructure. The governance of city-wide telecommunications digital twins — determining who owns the data, who controls access to the model, and how the data is protected — requires careful legal design that addresses the competing interests of municipal authorities, telecommunications operators, residents, and technology platform providers.

The data protection implications of city-wide telecommunications digital twins — specifically the processing of location and usage data about individual residents that is incorporated into the digital twin model — require careful analysis under the DPDPA's framework. Location data derived from cell tower connections (showing residents' movements through the city) is personal data that can reveal sensitive information about individuals' activities, associations, and habits. The use of this data in a city-wide digital twin — even in aggregated form — must be justified under a lawful basis (such as the legitimate interest of optimising telecommunications infrastructure, or compliance with the operator's licence conditions requiring specific quality of service standards in specific areas) and must comply with data minimisation requirements (using the minimum level of granularity and identifiability needed for the specific analytical purpose). The development of privacy-preserving digital twin architectures — using techniques such as differential privacy, federated learning, and synthetic data generation to enable useful city-level analytics without processing individually identifiable data — is an active area of research and regulatory development that India's telecommunications and data protection regulatory frameworks should actively encourage.

G.4 Looking Forward: Closing Reflections

India's telecommunications and digital economy legal framework in 2024 and beyond represents the product of three decades of market liberalisation, regulatory development, judicial interpretation, and technological transformation that has produced one of the world's most complex and dynamic regulatory environments. The Telecommunications Act, 2023's enactment marks both a culmination — of the long process of replacing the 1885 Act — and a beginning: the start of a new era of regulatory implementation and jurisprudential development that will determine whether the Act's ambitious framework for connectivity, security, and digital rights is realised in practice. For legal practitioners working in this space — advising telecom operators, technology companies, investors, regulators, and government — the mastery of this framework requires both deep knowledge of the specific rules and precedents and a broader understanding

of the constitutional, economic, and technological context in which the rules operate. The most important insight for practitioners is that telecommunications regulation is not static: it is a continuously evolving body of law shaped by technological change, market evolution, regulatory learning, and judicial development, and effective advice requires ongoing engagement with this evolution rather than reliance on fixed knowledge.

The convergence of telecommunications law with data protection law, competition law, cybersecurity law, and digital economy regulation creates both challenges (managing multiple overlapping frameworks) and opportunities (developing integrated legal expertise that spans the full range of digital governance issues). The practitioners who will be most valuable to their clients in the coming decade are those who can navigate this complex regulatory landscape with both technical credibility (understanding the technology that regulation governs) and legal rigour (applying constitutional and statutory analysis to novel regulatory questions). The Telecommunications Act, 2023 — with its broad mandate, its constitutional grounding, and its implementing rules still to be developed — is the foundation on which this new generation of digital law practice will be built. The task ahead is large, the stakes are high, and the opportunities — for practitioners, for India's digital economy, and for the hundreds of millions of Indians who will benefit from well-governed, affordable, secure, and rights-respecting telecommunications — are immense. Bhatt and Joshi Associates commend this series of booklets as a contribution to the ongoing development of India's telecommunications law practice and look forward to the continuing evolution of this vital field.

SUPPLEMENTARY NOTE H

Digital Economy: Final Perspectives

H.1 Platform Governance and Telecom

The emergence of dominant digital platforms — entities such as the major social media networks, messaging applications, e-commerce marketplaces, and cloud computing services that have achieved market positions of significant market power — creates governance challenges that extend to the telecommunications sector in several specific ways. First, telecommunications operators must interconnect with major digital platforms to provide their subscribers with access to platform services: the quality and terms of this connectivity (which is critical for subscriber experience) are influenced by the commercial negotiations between operators and platforms. Second, telecommunications operators' own digital services — such as mobile payments, entertainment content, and cloud storage — compete in markets where major

platforms hold dominant positions, raising competition law questions about platforms' treatment of competing operator services. Third, major platforms' use of telecommunications infrastructure for their own communication services (WhatsApp, Google Meet, Zoom) raises the OTT regulation question that has been a persistent feature of India's telecommunications regulatory agenda. Fourth, platforms' data processing activities — which rely on the personal data of telecommunications subscribers — create a data governance dimension that connects platforms' activities directly to the telecommunications sector's DPDPA obligations.

India's approach to digital platform governance — as reflected in the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the proposed Digital Competition Bill (which has been under development), and the Competition Commission's market studies on digital platforms — is developing a regulatory framework that seeks to address platform market power without stifling innovation. The digital competition framework — likely to be enacted as standalone legislation alongside the Competition Act amendments — would impose ex ante obligations on "systemically significant digital enterprises" (SSDs) including: fair and non-discriminatory treatment of third-party businesses using the platform (preventing self-preferencing); data interoperability (enabling users to transfer their data between platforms); transparency about ranking, recommendation, and algorithmic curation (addressing opacity in how platforms select and present content); and restrictions on anti-competitive acquisitions (preventing dominant platforms from acquiring potential competitors before they become significant threats). These platform governance obligations have direct relevance for the telecommunications sector, since major operators with significant digital platform businesses (Jio's digital ecosystem, Airtel's content and cloud offerings) may be classified as SSDs subject to digital competition obligations alongside their standard telecommunications regulatory requirements.

The relationship between telecommunications regulation and platform governance creates specific challenges for the design of both regulatory frameworks. Telecommunications regulators (TRAI, DoT) have expertise in network technology, spectrum management, and consumer protection for connectivity services but limited experience with platform market economics and digital market conduct. Competition regulators (CCI) and digital market regulators (MeitY) have expertise in competition law and digital governance but limited technical expertise in telecommunications network management and spectrum policy. The effective governance of the telecommunications-platform interface — addressing issues that span both domains, such as the net neutrality implications of platform interconnection arrangements, the competition implications of operator-platform exclusive arrangements, and the data governance implications of

telecom-platform data sharing — requires institutional cooperation and potentially joint regulatory capacity development across these bodies.

H.2 Quantum Communications: Regulatory Horizon

Quantum communications technology — which uses the principles of quantum mechanics to transmit information in ways that are fundamentally secure against eavesdropping — represents the most profound potential disruption to the telecommunications security landscape since the development of public-key cryptography in the 1970s. Quantum Key Distribution (QKD) — the most mature quantum communications technology — uses quantum properties of light to distribute cryptographic keys between two parties in a way that any eavesdropping attempt leaves a detectable signature, enabling the detection of any interception of the key. While QKD is not yet commercially deployed at scale, India's National Quantum Mission — with its Rs. 6,000 crore investment in quantum technology development — includes significant R&D; programmes for quantum communications that are expected to produce deployable quantum communications systems within the mission period. The regulatory framework for quantum communications — governing the deployment of quantum network infrastructure, the certification of quantum communications equipment, and the integration of quantum security with existing telecommunications networks — must be developed in advance of commercial deployment to avoid creating regulatory uncertainty that delays adoption.

The regulatory challenges of quantum communications include: spectrum management (QKD using optical fibre does not require spectrum, but quantum repeater networks and free-space QKD systems may require specific optical frequency coordination); equipment certification (quantum communications equipment must be certified against security standards that address the specific vulnerabilities of quantum systems, including side-channel attacks on quantum hardware); network integration (the integration of quantum secure channels with existing encrypted telecommunications networks requires clear standards for the interfaces and cryptographic protocols that bridge quantum and classical security); and international coordination (QKD-secured international communications links require both technical standardisation and diplomatic agreement on the use of quantum communications infrastructure). India's National Quantum Mission provides the R&D; foundation for developing domestic quantum communications capability; the development of the complementary regulatory framework — through TEC standards development, WPC spectrum planning for quantum communications, and international standards engagement — is an equally important priority for ensuring that India's quantum communications investment translates into commercially deployable, regulatory-compliant quantum communications infrastructure.

H.3 Long-Term Regulatory Trajectory

The long-term trajectory of India's telecommunications regulatory framework — over the decade from 2025 to 2035 — will be shaped by several converging trends that practitioners and policymakers must understand and anticipate. The technological convergence of terrestrial mobile, satellite, and fixed broadband networks into a single integrated connectivity platform — enabled by 6G's NTN integration and by the increasing capacity of LEO satellite constellations — will require a correspondingly converged regulatory framework that addresses all access technologies under a unified framework of obligations and standards. The economic convergence of telecommunications and digital platform services — as operators increasingly provide digital services alongside connectivity, and as digital platforms increasingly invest in connectivity infrastructure — will require regulatory frameworks that address both telecommunications and digital economy aspects of converged service offerings. And the geopolitical convergence of digital technology, national security, and economic competition — as countries use digital infrastructure as an instrument of strategic competition — will require telecommunications regulatory frameworks that are explicitly aligned with India's national security and economic development objectives.

The practitioners of the future in India's telecommunications law will operate in a regulatory environment of extraordinary complexity and rapid change, requiring expertise that spans technical telecommunications, constitutional law, competition economics, data protection, cybersecurity, and digital platform governance. The development of this multidisciplinary expertise — through legal education, continuing professional development, and the collaborative development of interdisciplinary practice groups — is a professional responsibility for the Indian legal community and a competitive advantage for law firms and legal departments that build it proactively. Bhatt and Joshi Associates' commitment to maintaining leading-edge expertise in India's telecommunications and digital economy law — through continuous learning, expert engagement, and the publication of reference materials such as this booklet series — reflects the firm's understanding that the quality of legal advice in this domain depends on the depth and currency of the practitioner's regulatory knowledge. The Telecommunications Act, 2023 and the regulatory architecture that develops under it will be the framework within which India's digital future unfolds; the legal practitioners who master this framework will be essential partners in that unfolding.

SUPPLEMENTARY NOTE I

Digital Economy: Concluding Perspectives

I.1 The Future of Telecommunications Regulation

The future of telecommunications regulation in India — in the decade from 2025 to 2035 — will be shaped by the convergence of three transformative trends: the technology revolution of 5G, 6G, and AI; the geopolitical shift toward digital sovereignty and supply chain security; and the social and constitutional recognition of digital access as a fundamental right. The technology revolution will fundamentally change what telecommunications networks do and how they do it: 5G and 6G networks will be intelligent, programmable platforms that enable an almost unlimited range of applications rather than simple connectivity pipes; AI will be embedded throughout network operations, customer service, and security management; and the boundary between telecommunications and computing will dissolve as edge computing becomes integral to network architecture. The geopolitical shift will require telecommunications networks to be designed and governed with national security considerations as a primary constraint: supply chain security, data sovereignty, and the strategic alignment of digital infrastructure with democratic values will be regulatory requirements as much as commercial choices. And the constitutional recognition of digital access as a right will require the regulatory framework to ensure that connectivity is universally accessible and affordable, not merely commercially available.

The regulatory institutions that govern India's telecommunications sector — TRAI, DoT, TDSAT, CERT-In, WPC, and their inter-agency coordination mechanisms — must evolve to match the complexity of the regulatory challenges ahead. TRAI will need significantly expanded technical capacity (in AI, quantum communications, satellite systems, and spectrum sharing technologies) alongside its existing expertise in market analysis, consumer protection, and regulatory economics. TDSAT will need enhanced capacity for managing complex, technically intensive proceedings and for keeping pace with the rapidly evolving body of telecommunications regulatory law being developed under the 2023 Act. CERT-In will need expanded capabilities in AI-assisted threat detection, quantum-safe cryptography assessment, and international cooperation to address the increasingly sophisticated and globally coordinated cybersecurity threats targeting India's telecommunications infrastructure. And the coordination mechanisms between these institutions — which have historically been ad hoc and informal — will need to be formalised and strengthened to manage the complex multi-jurisdictional regulatory questions that the converging telecommunications and digital economy landscape will increasingly present.

The practitioners who serve India's telecommunications regulatory system — the lawyers, economists, engineers, and policy specialists who advise the regulated industry, represent parties in regulatory proceedings, and develop regulatory policy — play an essential role in the

quality and legitimacy of telecommunications governance. Effective legal practice in this domain requires both technical mastery (understanding the regulatory framework in sufficient depth to provide accurate and reliable advice) and institutional awareness (understanding how regulatory decisions are actually made, how TDSAT proceedings actually function, and how the relationships between regulatory actors shape regulatory outcomes). This booklet series — covering the Telecommunications Act, 2023, TRAI's regulatory architecture, the spectrum and licensing framework, TDSAT's jurisprudence, cybersecurity and data protection, and the digital economy's emerging legal landscape — is intended as a contribution to that technical mastery and institutional awareness. Bhatt and Joshi Associates commend these materials to practitioners, students, and others who engage with India's telecommunications legal landscape and welcome the ongoing professional dialogue that keeps this complex and vital field of law at the forefront of India's legal practice.

SUPPLEMENTARY NOTE J

Digital Economy: Closing Remarks

J.1 The Digital India Vision and Telecommunications Law

The Digital India initiative — the government's flagship programme for transforming India into a digitally empowered society and knowledge economy — provides the overarching policy context within which India's telecommunications regulatory framework must be understood and evaluated. Digital India's three core components — digital infrastructure (high-speed internet connectivity, common service centres, cloud computing infrastructure), digital governance (online government services, paperless transactions, digital identity), and digital literacy (training citizens to access and use digital services) — all depend critically on the telecommunications regulatory framework to create the conditions for universal, affordable, and reliable digital connectivity. TRAI's regulatory decisions about mobile broadband pricing, quality standards, and coverage obligations directly determine whether the connectivity component of Digital India can be realised; DoT's spectrum management policies determine whether the network capacity and coverage needed for Digital India applications is available; and TDSAT's enforcement of regulatory standards ensures that the connectivity commitments made by operators translate into actual subscriber experience. The alignment between India's Digital India objectives and its telecommunications regulatory framework — specifically ensuring that the regulatory framework creates conditions for the connectivity quality and affordability that Digital India requires — should be an explicit criterion in all major telecommunications regulatory decisions.

The rural connectivity dimension of Digital India — the specific challenge of extending meaningful, affordable internet connectivity to India's 800 million rural residents — requires a telecommunications regulatory framework that goes beyond the urban commercial market focus that has historically dominated regulatory attention. The BharatNet programme — the government's initiative to provide optical fibre connectivity to all 250,000 gram panchayats in India — has provided the backbone infrastructure for rural connectivity, but the last-mile challenge (connecting individual households and community centres to the BharatNet fibre) remains substantial. The telecommunications regulatory framework can support last-mile rural connectivity through: right-of-way facilitation for rural network deployment (reducing the cost and time required to deploy infrastructure in rural areas); spectrum availability for rural coverage (ensuring adequate spectrum is available for rural mobile broadband coverage); Digital Bharat Nidhi support for rural last-mile investment (subsidising deployments that are not commercially viable without support); and enabling non-commercial community network deployments (facilitating the deployment of community-owned connectivity infrastructure in areas where commercial operators have no incentive to invest). Each of these regulatory interventions has a legal dimension — right-of-way rules, spectrum assignment conditions, DBN programme guidelines, and community network licensing frameworks — that requires careful design and implementation under the Telecommunications Act, 2023's framework.

The long-term vision of universal digital access for India — in which every Indian, regardless of geographic location, income level, gender, or disability status, has access to affordable high-quality internet connectivity and the digital literacy needed to use it productively — is both an economic objective (enabling the full participation of all Indians in the digital economy) and a social justice imperative (ensuring that the benefits of digital transformation are not concentrated among the already-advantaged segments of society). The telecommunications regulatory framework is not the only instrument for achieving this vision — digital literacy programmes, public access facilities, affordable device availability, and relevant local content are all essential complements — but it is a foundational one: without the right regulatory conditions for connectivity infrastructure deployment, pricing, and quality, no other programme can fully achieve universal digital access. The practitioners and policymakers who work within India's telecommunications regulatory framework carry a significant responsibility for how it is designed and implemented — a responsibility whose ultimate measure is whether it contributes meaningfully to the realisation of universal digital access for all Indians, and through that, to India's broader vision of an inclusive, prosperous, and digitally empowered society.

SUPPLEMENTARY NOTE K

Digital Economy: Closing Thoughts

K.1 Building India's Digital Infrastructure Law

The development of a comprehensive, coherent, and constitutionally grounded legal framework for India's digital infrastructure — encompassing telecommunications regulation, data protection, digital platform governance, cybersecurity, AI governance, and space communications — is one of the most important legal governance tasks of the current era. The Telecommunications Act, 2023, the DPDPA, 2023, the evolving IT Act framework, the proposed Digital Competition Act, and the emerging AI governance framework are the building blocks of this comprehensive digital infrastructure law. The coherence of these building blocks — their consistency with each other, their alignment with India's constitutional framework, and their adaptability to technological change — will determine whether India's digital governance architecture serves as a robust foundation for the country's digital development or becomes a source of regulatory fragmentation and legal uncertainty. The practitioners, academics, policymakers, and judges who work with this body of law carry a collective responsibility for developing it thoughtfully, consistently, and with attention to its constitutional underpinnings and its real-world consequences for the hundreds of millions of Indians whose digital lives it governs.

The international dimension of India's digital infrastructure law — its alignment with or divergence from international standards and frameworks — will increasingly matter as India integrates more deeply into the global digital economy. Indian companies that operate in international markets must comply with multiple national regulatory frameworks; international companies that operate in India must meet Indian regulatory requirements that may differ from their home market requirements. The development of India's digital infrastructure law in ways that maximise alignment with international best practice — while appropriately reflecting India's specific constitutional framework, national security requirements, and development priorities — would reduce compliance costs, facilitate digital trade, and strengthen India's position in global digital governance discussions. TRAI, DoT, MeitY, and other regulatory agencies should systematically assess the international dimensions of their regulatory decisions, seeking alignment with international standards where appropriate and explaining deviations where India's specific circumstances justify a different approach.

The ultimate purpose of India's digital infrastructure legal framework — including the telecommunications regulatory architecture described throughout this booklet series — is to create the conditions under which India's digital potential can be fully realised: a digital economy that is dynamic, innovative, inclusive, and secure; digital infrastructure that is resilient, affordable,

and universally accessible; and digital governance that respects fundamental rights, maintains the rule of law, and serves the public interest. Achieving this purpose requires not only well-designed regulatory frameworks but strong institutions to implement them, professional legal communities to interpret and apply them, and an informed public to hold both institutions and industry accountable for their performance. Bhatt and Joshi Associates is honoured to contribute to this ecosystem through its legal practice and through publications such as this booklet series, and remains committed to the ongoing development of India's telecommunications and digital economy legal landscape in service of these fundamental objectives.

FINAL NOTE: The Digital Future — A Legal Perspective

The digital future that India's telecommunications and digital economy legal framework is helping to shape is one of extraordinary opportunity and significant risk. The opportunity is unprecedented: for the first time in human history, it is technically and economically feasible to provide every person on earth with access to the accumulated knowledge, creative output, and communicative capacity of humanity — and India's telecommunications regulatory framework, properly designed and implemented, can make this possibility a reality for India's 1.4 billion citizens. The risk is equally significant: digital connectivity creates new vulnerabilities — to surveillance, manipulation, fraud, and exclusion — that can harm the most vulnerable members of society disproportionately if the governance framework does not protect them adequately. The central challenge of digital governance is managing this tension between opportunity and risk in a way that maximises the benefits of digital connectivity while effectively mitigating its harms. The Telecommunications Act, 2023, the DPDPA, 2023, and the evolving digital governance framework collectively represent India's response to this challenge — a response that is still developing and that will be shaped by the regulatory decisions, judicial interpretations, and policy choices of the coming decade.

The legal dimension of India's digital future is not merely about compliance and enforcement — it is about the constitutional values that the legal framework embodies and the social vision it serves. A telecommunications legal framework that genuinely respects the privacy rights recognised in Puttaswamy, the internet access rights recognised in Anuradha Bhasin, and the equal protection rights guaranteed by Article 14 will create a digital environment that is safer, more inclusive, and more conducive to human flourishing than one that treats rights protection as a secondary consideration to commercial and security objectives. The practitioners, scholars, regulators, and judges who develop and apply India's telecommunications law carry a responsibility not only for its technical correctness but for its fidelity to these constitutional values — a responsibility that is ultimately discharged not in legal documents and regulatory orders but

in the digital lives of the hundreds of millions of Indians whose connectivity, privacy, and freedom of expression depend on getting the law right.

Bhatt and Joshi Associates presents this final booklet in the series — covering OTT services, satellite communications, 5G, and India's digital economy future — as a contribution to the legal and regulatory knowledge that practitioners in this field require. The six booklets in this series collectively cover the full legal landscape of Indian telecommunications law as reshaped by the Telecommunications Act, 2023: from the constitutional framework and statutory architecture of Booklet I, through the regulatory and adjudicatory institutions of Booklets II and IV, the spectrum and infrastructure framework of Booklet III, the cybersecurity and data protection framework of Booklet V, and the digital economy's emerging legal challenges addressed in this booklet. Together, these booklets aim to provide both the foundational knowledge and the analytical framework needed for sophisticated legal practice in India's telecommunications and digital economy. The firm welcomes feedback from practitioners, clients, and colleagues on any aspect of these materials and looks forward to updating them as India's telecommunications legal landscape continues to evolve.

The development of India's digital trade framework — the legal and regulatory arrangements that govern the cross-border flow of digital services, data, and digital infrastructure investment — is closely connected to the telecommunications regulatory framework and will increasingly shape the commercial environment for telecommunications and digital economy operators. India's engagement with digital trade in international forums — the WTO's e-commerce negotiations, the G20's digital economy framework, and bilateral digital trade agreements with strategic partners — will progressively create legal commitments about the regulatory treatment of digital services (including telecommunications services and OTT communication services) that constrain India's domestic regulatory discretion. Understanding the interaction between India's WTO telecommunications commitments (under the GATS Fourth Protocol), its emerging digital trade commitments, and its domestic regulatory framework (under the Telecommunications Act, 2023 and the DPDPA) is an essential competency for practitioners who advise on cross-border telecommunications and digital economy transactions.

The evolution of digital payment systems — and specifically the integration of telecommunications billing with financial payment systems — creates important regulatory interfaces between telecommunications regulation and financial regulation that practitioners must understand. India's UPI platform, which enables mobile-based real-time payments using phone numbers as payment identifiers, creates a direct link between the telecommunications subscriber's mobile number (managed under the telecom regulatory framework) and their

financial identity (managed under the financial regulatory framework). Security vulnerabilities in the telecommunications system — such as SIM swap attacks, SS7 vulnerabilities, or mobile number portability fraud — can directly compromise the financial security of subscribers who use UPI and other mobile-based payment systems. The coordination between TRAI, DoT, and RBI on the security requirements for telecommunications systems that are integrated with financial payment infrastructure is therefore a critical regulatory governance priority that requires cross-sectoral collaboration at the highest levels of both regulatory authorities.

India's position in the global digital economy — as both a major consumer market for digital services and a significant producer of digital technology, software, and services — gives it a unique dual perspective on digital governance that should inform its regulatory framework for the telecommunications and digital economy sector. As a consumer market, India needs regulatory frameworks that ensure affordable, high-quality, and rights-respecting digital services for its population. As a technology producer, India needs regulatory frameworks that create a supportive environment for the development and export of Indian digital technologies, including telecommunications software, security solutions, and digital public infrastructure components. The design of India's telecommunications regulatory framework should explicitly account for both perspectives — creating conditions that serve India's domestic consumers while also supporting India's ambitions as a global digital technology and services exporter. This dual perspective — consumer market and technology producer — is the lens through which India's most sophisticated telecommunications regulatory practitioners and policymakers approach their work, and it is the lens through which this booklet series has been developed.