Unpacking the Key Costs and Consequences of the New Telecom Bill

aapti institute

Unpacking the Key Costs and Consequences of the New Telecom Bill

March 2023

aapti institute

Kunal Raj Barua, Mousmi Panda & Dr. Sarayu Natarajan

Authors

Aapti is a public research institute that works on the intersection of technology and society. It examines the ways in which people interact and negotiate with technology both offline and online.

contact@aapti.in aapti.in

Financial disclosure: This research study was undertaken by Aapti Institute, an independent public research think tank, and was sponsored by Google India. The research output has been independently generated and without external influence. It was produced through discussions with policy experts, academicians, and industry and legal experts.

Index

1. Executive Summary

India's thriving digital economy and increasing citizen participation in the digital world has compelled regulation of the sector. In late 2022, the government introduced the Indian Telecommunication Bill with the objective of consolidating telecommunication legislation, addressing sectoral growth and prioritizing user safety with newer technological advancements. The bill proposes an expansive definition of 'telecommunications services' by bringing Over-The-Top (OTT) communication services under the Department of Telecommunications (DoT) regulatory net, resulting in various potential economic and non-economic implications and costs for citizens, businesses, and the government itself.

The study unpacks these implications for users, businesses and the government, and highlights the resultant impact. In its current form, the report finds notable financial and non-financial costs for the mentioned stakeholders. In the study, users refers to any users of telecommunication services, businesses refers to OTT platforms and traditional telecommunication services providers, unless mentioned separately, and the government refers to the bodies that regulate and govern the telecommunication industry.

The research also finds the possibility of second-order consequences - first, the bill could increase hesitancy from users due to increased friction and resource spending, and issues of user safety, privacy, affordability and accessibility could remain unaddressed. Second, business entities could incur compliance costs - which have implications on model types - thereby needing to add features just to be compliant. This could reduce the impetus to improve the quality of services and user interfaces.

These costs, unpacked further in the study, therefore run the risk of increasing costs for the entire ecosystem. An attempt to uniformly regulate heterogeneous models would serve as an encumbering force. While the intent of the bill is well-founded, the escalation of costs could increase ecosystem friction - resulting in resource drains from all sides.

The report finds that an improved understanding and articulation of service models could benefit the relevant stakeholders in providing, using, and regulating services, and suggests the need for streamlined regulation.

For this paper, desk research was supplemented by 10 interviews with academicians, industry leaders and experts. The detailed study can be found here.

The following diagram illustrates the key costs identified along the various stages of the business journey that could be incurred by entities providing telecommunication services.

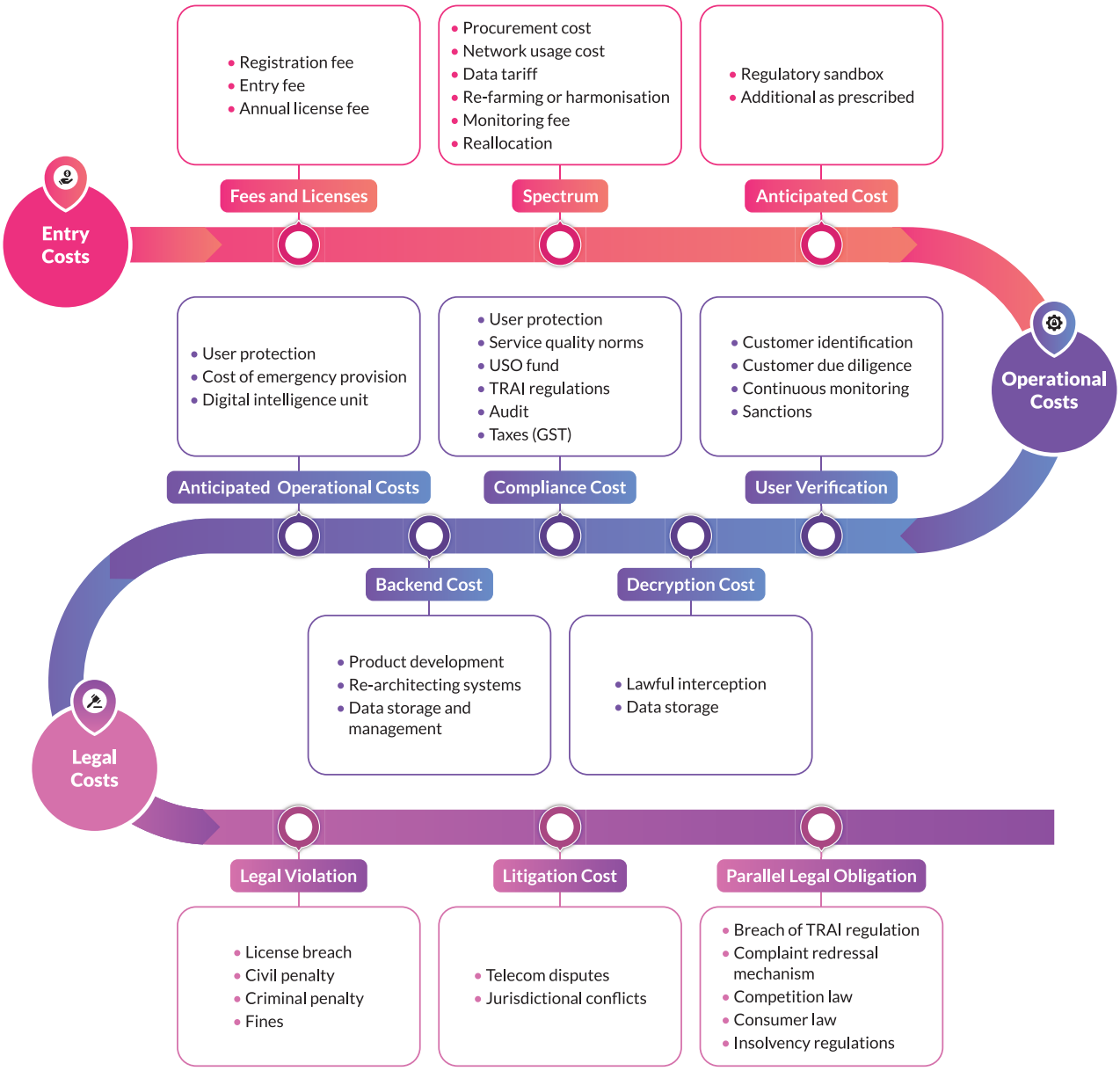
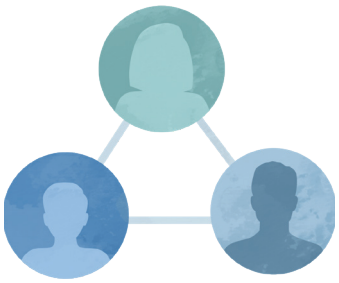


Figure 1: *Journey of a telecommunication service under the proposed Indian Telecommunications Bill*

1.1 Potential Costs for Stakeholders Under the Bill

Business entities could potentially incur recurring expenditure such as license and other fees, contributions to the Telecommunication Development Fund (TDF), costs of communication, and additional network charges. Entities could experience sizeable capital and operational costs to modify processes and technology for user verification, decreased encryption, data sharing and data management. Additionally, entities could face significant costs to be consistently compliant and face a range of legal expenses in case of any breach. These costs could result in platforms losing users, dispensing with key privacy features, increased friction with regulatory bodies, and stagnation regarding innovation to adhere to compliance.



Users could experience reduced affordability as platforms shift to freemium models, higher data tariffs, fewer platform options, and increase in resource costs for user verification. Small businesses could also incur basic operational costs if they continue using such platforms. Users could be subjected to fines in case of misrepresentation of information, leading to increased hesitancy in the case of users with low literacy levels. The new provisions also raise concerns around the privacy and management of users' personal information and communications, and could create friction between users, service providers and the government.

The **government** is not immune and could incur significant costs to ensure compliance and maintain technological infrastructure. Capacity building of regulatory and legal departments (DoT, Telecom Regulatory Authority of India, Telecom Disputes Settlement and Appellate Tribunal), conducting technological audits, and monitoring a large pool of service providers could invite more resource expenditure. Regulating entities would require efficient cross-sector capacity building and could even lead to confusion when determining national jurisprudence, in addition to maintaining geo-political sensitivities for global service providers.

1.2 Proposed Recommendations and Considerations

There are three main recommendations:

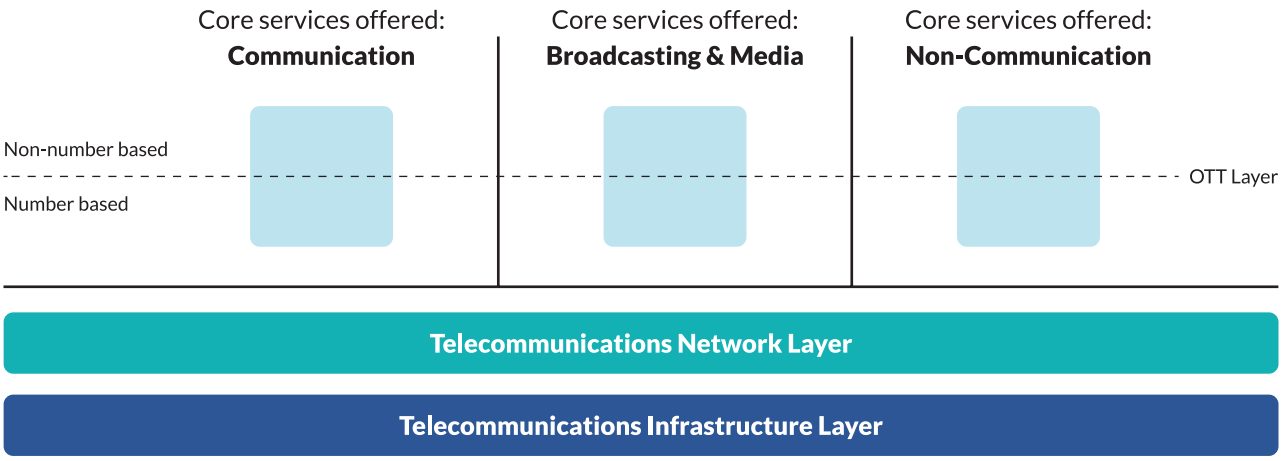


Figure 4: *Proposed framework to classify service models*

- First, **clear taxonomy and structured definitions** would allow for more balanced and efficient regulation. To that extent, classification of services based on layer and core offering type with clear distinctions between network operators and OTT platforms may be considered.
- Second, to enhance user protection, **differentiation of regulation and clear mapping of regulatory bodies** to entities enable lowering of entry barriers for new entrants.
- Third, **balancing national security** around telecommunications requires protocols on efficient data management, transparency around entity contributions, and practices relating to data and user safety with improved access and privacy for underserved populations.

Due to the integral nature of the telecommunications industry in the Indian and digital economy, the private and public sectors need to work collaboratively to improve ecosystem understanding of model types and pathways to improve service delivery and create efficient data safety and management protocols while balancing user and national security. The study also highlights the need for collaboration to improve resource sharing, ease of conducting business, improved quality of service, user protection, affordability, and user literacy.

2. Introduction

It is strikingly evident that India's ascension to the world stage over the past few decades has been fueled by its vibrant digital economy. This year, 2023 — the year of India's G20 presidency — is witnessing several initiatives to streamline and unify regulation in this space. Structuring a safe, thriving digital economy is critical as the next half-billion of India's citizens enter the digital world. In India's techade, having meaningful regulation that puts India and Indians first is essential.

To that end, the Department of Telecommunications of the Ministry of Communications released a draft bill, the **Indian Telecommunication Bill**, on September 21, 2022[1] with the objective of bringing telecommunication legislation on a par with growth in the sector and the industry at large — in consonance with the advancements in technology and its usage. The bill is aimed at reducing the multiplicity of laws[2] governing telecommunications by consolidating them into this piece of legislation[3].

Among other things, the bill expands the definition of 'telecommunications services', thereby bringing a host of service providers under the regulatory umbrella of the Department of Telecommunications (DoT) and the Telecom Regulatory Authority of India (TRAI), imposing possible economic obligations, and placing additional obligations on 'telecommunication service providers' (TSPs).

How can the bill achieve a balance between ensuring protection and safety of its legitimate interests, on the one hand, and fostering innovation, on the other? To identify the parameters for the former, this paper explores the potential monetary and non-monetary costs of this legislation, and their implications on citizens, businesses, and the government itself. We look forward to this study[4] fostering a deep conversation in the right direction to regulate India's burgeoning digital economy.

This report finds that users, businesses, and the government will likely experience increased monetary and non-monetary costs as a consequence of the proposed legislation. Accordingly, the report recommends some key measures - exploring a more structured approach for the classification of entities - separating telecom providers from OTT providers, internet-based and interpersonal communication services, exploring mechanisms for minimum efficient regulation, and exploring collaborative practices of data management to balance national security with secure communications. Cumulatively, these measures could add to the already planned supportive regulation for the digital economy, in turn fostering greater trust and engagement.

The research looks to provide a comprehensive understanding of the bill from the lens of monetary and non-monetary implications. In doing so, it hopes to unify taxonomy relevant to the ecosystem and provide key stakeholders a collective starting point to dive deeper. A further exploration by quantifying the costs and mapping attribution would be beneficial to this sector.

The paper is structured as follows: The subsequent section examines the need for the study from the perspective of users, businesses, and government. The section after attempts to map, stakeholder-wise, the cost implications of the bill. The aim of this segment is to identify and map the potential costs of the bill and, secondarily, its implications on the digital economy. The following section examines the resultant need for definitional clarity. The concluding section details areas for consideration.

2.1. The need for this study

In the past decade, businesses have flourished, and users have been able to leverage affordable and accessible digital solutions. With such growth, the responsibility of ensuring safety lies with the government. This study hopes to understand how these key actors are likely to experience various costs and consequences, and accordingly peruses their concerns and the various ways these costs might impact the ecosystem.

[1] Indian Telecommunications Draft Bill
[2] Three acts governing the telecommunications industry are: (i) the Indian Telegraph Act, 1885 ; (ii) the Indian Wireless Telegraphy Act, 1934 ; and (iii) the Telegraph Wires (Unlawful) Possession Act, 1951.
[3] Explanatory note to the draft Indian Telecommunication Bill
[4] Appendix 1

3. Service Providers Incur Various Costs That Have Monetary and Non-Monetary Implications on Stakeholders

3.1 IMPACT ON BUSINESSES

With India's economy being fueled by a vibrant and competitive market, introduction of new costs could impact innovation, and ease of doing business for OTT service providers and other telecommunication services. To continue promoting high quality service provision and foster a supportive ecosystem for innovation, it is key for stakeholders to understand the potential implications that might arise from such proposed regulations. This understanding could encourage regulators in initiating the desired equilibrium between user protection and market growth and achieving the goal of a trillion dollar digital economy.

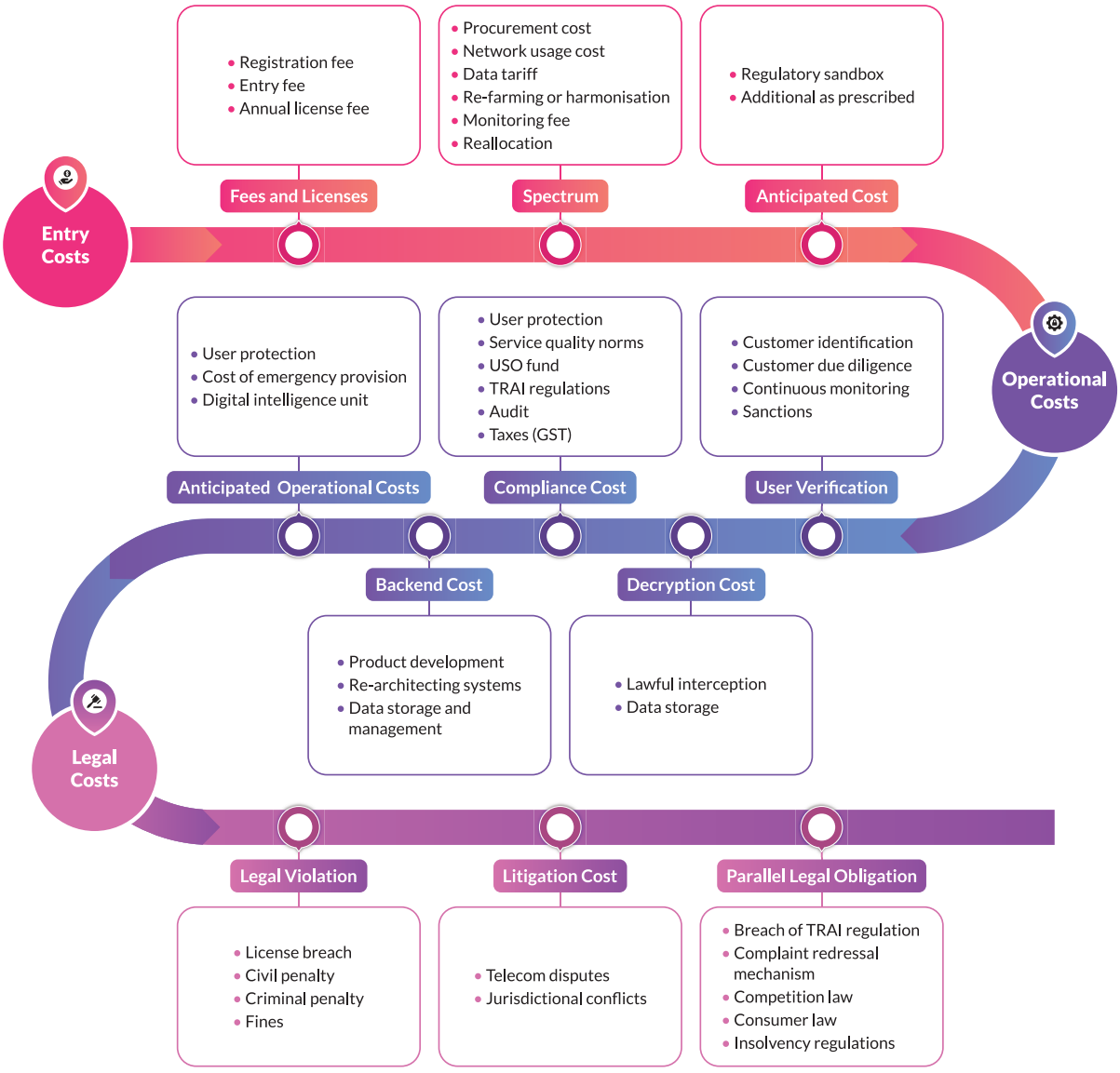


Figure 1: *Journey of a telecommunication service under the proposed Indian Telecommunications Bill*

This section highlights the key costs that could be incurred by businesses and the impact this might have on other stakeholders.

3.1.1 Licenses and Fees

Licensing and renewal are significant recurring cost for businesses. Apart from being an issue of monetary concern, the licensing provisions also expose businesses to stricter terms and conditions, the breach of which can result in various penalties or subjection to suspension, curtailment, and revocation. Increased scrutiny requires determining business models; capacity building of policy teams; and reduced time and capital to improve the quality of services. The uncertainty around the licensing and fees could affect collaborations, crossovers, and business investment pipelines.

The license is a significant authoritative regulatory instrument with cumbersome processes[5]. Implicit costs include registration with the procurement of certified telecom infrastructure, and auditing[6]. Furthermore, entities could incur additional costs under the Minimum Requirements for Security Policy of DoT licensees[7] for which an empaneled third-party[8] "information security audit" is required — with the cost being borne by the entity[9].

The security policy provides direction for the establishment, implementation, maintenance and continual improvement in Security and Security Management for licensees. This tertiary upkeep and updating cost are applicable to telecom networks and systems holding customers' data including the endpoints through which such infrastructure and information can be made accessible[10] to relevant entities.

3.1.2 Telecommunication Development Fund (TDF)

Section 28 of the bill mandates a contribution towards the TDF. The share and allocation for contribution remains undefined but for the TSPs, 5% goes to the Universal Service Obligation Fund (USOF) and 3% to the general exchequer[11] of the total 8% adjusted gross revenue (AGR). Experts have called this an unnecessary financial obligation that has failed to meet its objective[12] and questions around the TDF utilization[13] remain unanswered.

3.1.3 Network Usage Costs

Service providers might need to pay annual charges which can be modified over time. Historically, TSPs have had to pay for spectrum allotment and comply with instructions of the licensor[14]. These charges for telcos have been scrapped for auctions held after September 15, 2021, and brought them financial relief.

Even though there is no explicit mention of network usage costs in the bill, recent developments[15] indicate that the DoT is keen to take a decision on revenue sharing after joint consultation with the telcos and the OTT players on the same. Therefore, the future application of such charges cannot be ruled out, given the persistent demand for OTTs to pay for their network usage costs. This could mean an additional cost burden on the OTT communication service providers, that could be imposed on top of the license fees.

Experts stated that this could have future implications where OTT platforms might need to incur significant costs for network procurement. Consultations to understand possible implications on spectrum sharing are ongoing[16] with additional research being conducted on how to make costs efficient for all stakeholders[17] in the telecom space. Experts highlighted that spectrum is only needed by mobile network operators[18] and have asked for functional separation of telecommunication layers through a network slicing approach.

[5] Aapti primary research and journey framework
[6] Aapti's primary and secondary research
[7] Government of India letter
[8] Empanelled under the 'Indian Computer Emergency Response Team (Cert-in). Government of India - Audit requirements
[9] Indian Express
[10] Aapti secondary research
[11] The Financial Express
[12] Aapti primary research
[13] Factly+ Government of India analysis
[14] Wireless Planning & Coordination (WPC) Wing: Cl 18.3 of the Unified License Agreement
[15] inc42.com
[16] TRAI Infrastructure sharing
[17] BEREC Infrastructure Sharing
[18] Aapti primary research

3.1.4 User Verification costs

Telecommunication service providers might require identification of users[19] to be conducted before service provision[20] — revealing the identity of the user on OTT platforms and message senders[21]. Researchers state that solving this solely through the identity path may not be adequate[22]. Individual user verification is a significant capital and operating cost for business entities — increasing processes around identification, due diligence, data gathering, managing, and monitoring.

OTT platforms perform specific functions and do not have any inherent system of higher user verification. Increased user verification is a significant change in the technology and addition of various data fields[23] — further adding to highlighted costs. Penalties could also be imposed on entities unable to maintain such protocols[24]. Ensuring accuracy, de-duplicating and maintaining shareable data formats are additional costs.

Partnerships between entities could entail investment in both capital and human resources to allow interconnectedness, database sharing and information storage[25]. The requirement of technologically enabled devices has been highlighted by the TSPs' comments[26] on the consultation paper released by TRAI. Mandatory user verification further dilutes the salient features of communication platforms that prioritize user anonymity through encryption[27].

Unethical practices such as data leakage, data theft, sale of data, consequent harassment, and poor consent mechanisms in the absence of data protection frameworks could disproportionately impact users[28].

3.1.5 Interception Costs

The bill provisions interception for user safety and national security[29]. The interception of interpersonal communication has implications for businesses, users, and the government. In addition to user safety and privacy concerns, it adds a sizeable infrastructure cost. The process typically requires realigning architecture at a technical level[30] and rethinking interoperability between a central monitoring system (CMS) and law enforcement offices[31]. Redesigning encryption features could pose potential costs for service providers[32] as data management at this level requires the presence of complex architectures[33].

3.1.6 Compliance and Legal Costs

To operate and be compliant, requires strategic resource allocation, this section highlights potential costs that could be incurred by business entities[34].

Regulatory compliance costs

Includes consumer protection regulations such as service quality norms, interconnection, following strict terms and conditions, maintaining network security guidelines, and contributing to the TDF. These compliances become important from the perspective of operations, yet pose challenges due to associated penalties, fees, and sanctions. With different types of compliances, frequent audits will become necessary to review adherence to various regulations.

TRAI's power to levy fees and charges[35] allows continued issuance of tariff orders[36] like the Prohibition of Discriminatory Tariffs for Data Services. TRAI also has the legal authority to request information and the ability to conduct investigations with equipment service providers[37]. The TRAI Act gives additional power to address harmful market developments with respect to the class of licensees to abstain from predatory pricing, competition, long term development and regulation of fair market mechanisms[38]. This regulatory oversight over telecommunication services could now also

[19] Section 4(7)
[20] Airtel
[21] Section 4(8)
[22] Zhao, Chen, Li, Yang and Wang
[23] Aapti's primary and secondary analysis
[24] Schedule 3
[25] Aapti's primary research
[26] Calling Name Presentation (CNAP) Telecommunication Networks: TRAI CNAP consultation paper
[27] Business Standard
[28] Rest of World
[29] Clause 50, Draft Indian Telecommunication Bill, 2022
[30] Aapti primary research
[31] Aapti's primary and secondary analysis
[32] Aapti's primary research
[33] Agrawal, Nyamful
[34] Aapti's primary and secondary research
[35] Section 11(1)(c)
[36] TRAI issuance orders
[37] Section 12

apply on the OTT communication services, interpersonal and internet based communication services as per the bill. Incidentally, the bill has limited the recommendatory powers of TRAI under this bill, by allocating the powers of licensing and determining operational terms of conditions to the DoT.

Financial compliance costs

Includes conducting audits for the licensing costs, TDF fulfillment and other fees and charges. For telcos, financial reporting is a continuing cost as the license agreement requires the TSPs financial reports to be audited under the Companies Act, 2013, and mandates a report from the statutory auditor of the company. Under the new guidelines, the OTT communication service providers could also need to comply with the same financial reporting requirements. OTT platforms could now need to follow the license agreement terms and guidelines issued by DoT and TRAI to operate legally.

Data compliance costs

OTT communication platforms connect users globally, for interpersonal and business communication. The provision on user identity in the bill could grapple with international regulation, such as the General Data Protection Regulation (GDPR). To ensure global connectivity, navigating the international regulatory and compliance landscape could prove challenging due to conflicting laws. This could limit the ability of platforms to conduct business internationally. Finding the balance with multinational companies with incongruous laws between the entity's headquarter and connecting business in other jurisdictions could become intricate and create more confusion and entail possible future costs.

Jurisdiction related costs

The bill would bring OTT service providers under the additional jurisdiction of the DoT, apart from the already existing jurisdiction of the Ministry of Electronics and Information Technology (MeitY) and TRAI. Possible overlaps with competition law, consumer law, and insolvency and litigation legislation[39] could also occur. Defining OTT communication service providers as telecommunication services can bring the entities under the jurisdiction of the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) and open them to telecom disputes[40]. Other regulations like Consumer Protection, Interconnection Usage Charges, Consumers Education and Protection Fund, Standards of Quality of Service, and Commercial Communication Customer Preference could be applicable and have potential costs.

Litigation costs

The revenue sharing arrangement between the business entities often also leads to long-drawn litigation, such as between TSPs and DoT around the definition and calculation of AGR (Adjusted Gross Revenue)[41]. According to legal experts, these penalties are often substantial[42]. This is partly due to a lack of guidance around how penalties are structured and implemented[43]. Further, TSPs have historically been unwilling to pay these penalties, resulting in multiple rounds of litigation and increased counsel costs[44] — a burden that can fall on OTTs. The litigation costs could be triggered by alleged violation of the provisions, which tends to deter business entities due to escalated costs.

There can also be unanticipated legal costs as penalties for not following TRAI regulations such as license terms and conditions[45]. These are criminal and civil penalties and fines and can also extend to employees responsible to the company for the conduct of the business[46]. There are offenses such as providing services without license and contravention of any provision of licensing, and the penalties for breach of terms and conditions can range from written warning to a fine of up to ₹5 crore[47].

Softer laws such as best practices around cyber security are offset by hard laws such as Security Audit Certification of Web Portal and Websites[48] that telecommunication services providers must follow from time to time in the form of circulars and notifications[49].

Non-monetary implications like reputational damage and relationship friction could further impact the operations of business entities. The regulatory regime places an additional awareness burden and expectation of legal compliance. This translates into reduced efficiency for entrepreneurs and lack of commercial and operational flexibility to focus on innovation.

[38] Clause 46(k)
[39] Aapti's analysis
[40] Section 14
[41] Swarajya article
[42] Aapti primary research
[43] ibid
[44] ibid
[45] Clause 11, Schedule 3 & 4
[46] Clause 48
[47] Schedule 4
[48] TRAI memorandum: Audit certifications
[49] DoT circulars and notices

CASE STUDY

Understanding the impact of regulation on Other Service Providers (OSPs)

The OSPs industry has been regulated since 1999, till regulations were relaxed recently in 2021. As a bulk consumer of telecom resources, OSPs have to absorb heavy compliance obligations which were already being undertaken by telecom companies creating a double compliance burden on both the OSPs and TSPs.

The OSPs were subjected to documentation and financial, technical, and security conditions and penalties for breach. Such regulations resulted in burdening OSPs and resulted in monetary and non-monetary implications. These implications affected OSPs' ease of doing business and resulted in loss of competitive advantage and investment.

Figure 2: *Case study highlighting possible consequences of regulation*

3.2 IMPACT ON USERS

Though these identified areas primarily impact business entities, costs could be passed on to users, thus inhibiting access and affordability and impacting privacy. Furthermore, suspension of services without adequate provisions and guardrails in place could infringe on citizens' constitutional rights and freedoms. With goals to include more users into a safe and negotiable digital ecosystem through various schemes and market initiatives, increases in economic and non-economic costs could deter users from engaging in such spaces. This could lead to an uneven playing field and discourage users in the medium to long term.

3.2.1 Affordability

Addition of new costs could force entities to explore service-based subscription models — restricting access for users. Additionally, these costs might manifest for users in increased data tariff or subscription costs.

The fluctuating cost of data could also impact small businesses. Notably, such businesses have benefited from interpersonal communications platforms as they presented low-cost and easy to use solutions. Such platforms are being leveraged by approximately one million small sellers in India who use them for daily communication, business operations, customer communications and payment[50].

Socio-normative constraints further hamper access as smart devices and personal phones are often shared by family members and maintaining choice over such platforms could be further diluted. Research indicates that users often rely on their family member's digital literacy to complete verification processes, and this could further dilute the authenticity of the process, even resulting in misrepresentation by users and leading to penalties[51].

[50] Verloop.io
[51] Aapti's primary and secondary analysis

3.2.2 Awareness and access

With increased adoption of mobile devices, and a robust application marketplace, users have access to various platforms. Creating restrictions puts an added burden on users to be aware and continuously update themselves on telecommunication services lacking licenses[52]. MyGate provides community notice board messaging as its secondary services, however users might need to use various sources to acquire information which might have been previously unavailable.

The user verification process could become another hurdle as it commands users' time and resources and requires a certain level of digital literacy or convenient access to physical intermediaries to partake in the process. Additionally, socio-normative structures could discourage users from accessing such intermediaries and make the process laborious.

3.2.3 Privacy

Users are mandatorily required to disclose their identity or face penalties[53] to complete user verification. The mandatory verification provision can create hesitancy due to time and effort constraints and associated cost — furthering the digital divide[54]. With increase in the data collection process, users lack legal safeguards around how their information can be collected, managed, stored, and distributed. With stricter information and verification requirements for users, they might be unable to decide how much information they would like to share and truly understand consent mechanisms.

Reducing encryption features could further impact users in terms of content and information sharing with other users on platforms. With the interception clause, users might be fearful of how personal information is accessed, fueling further hesitancy. With users benefiting from previous data minimization protocols, the bill could potentially trigger a need for increased data collection.

3.3 IMPACT ON GOVERNMENT

During implementation, regulatory bodies could face various economic implications. The role of converging regulatory bodies could further confound the ecosystem, increasing costs. With the inclusion of new OTT services, singular authorities could incur significant costs to identify jurisdiction and subsequently allocate appropriate resources to address challenges.

This section identifies the various economic and non-economic costs that could be incurred by governments and other regulatory bodies.

3.3.1 Cost burden and capacity of government bodies and jurisprudence

The proposed regulations have notable implications for the government, requiring it to designate significant resources to ensure compliance. These could include utilization of continuous bandwidth of key government departments and officials, staff and auditors, and various other bodies to monitor legal and operational compliance.

Besides, the lack of a clearly defined stakeholder mapping exercise could result in continuous struggles to determine relevant authorities from a legal perspective. Without converging authorities present, identifying legal proceedings could lead to inefficient spending.

[52] Schedule 3
[53] Schedule 3
[54] Aapti's primary and secondary analysis

3.3.2 Regulation of 'all telecommunication services'

Regulatory framework that applies the same regulations for different types of services could become challenging. Different types of telecommunication services need to be classified based on their core functionality and other identifying attributes. With the encompassing definition, authorizing and permitting licenses could take up a bulk of regulators resources. Without determining core functionality, processes leading up to identification of model type could also result in pre-litigation costs. Similar to the discontentment expressed around AGR[55], relationships whilst regulating OTT services could also be severed.

3.3.3 Geopolitics of monitoring

The provision on lawful interception needs to prioritize citizens' perspective to escalate trust and reciprocate foreign relations. OTT communication service providers are part of the global communication chain and enforcing lawful interception can be a complex task, given the rights afforded to citizens by their respective nations. To maintain strong relations with other countries, authority regarding legislation will need to be decided at an international level in case of breaches and could entail significant cost.

3.3.4 Role of intermediary bodies and improved data management structures

Regulatory bodies such as the TRAI could require ongoing capacity building to be future-ready. Provisions such as user verification and lawful interception could lead to an unnecessary data deluge which would require adequate facilities to store and manage data. Creation and upkeep of technical and complicated architecture to incorporate interoperability would be yet another expenditure area.

Maintaining such large-scale databases and servers increases capital and operating costs for the government, requiring various consultative and technical processes to be put in place. Ensuring security of the collected data to minimize cyber-attacks is also imperative.

3.3.5 Improved protection protocols for citizens

In its attempt to be future-ready, the government must state the implicit consequences that could surface post-implementation. For instance, the government could incur expenses when putting in place data and purpose principles to safeguard the interests of the state and its citizens. Additionally, a more long-term solution needs to be devised to reduce reframing of legal provisions and readaptation to evolving technologies.

[55] Swarajya: AGR

4. Telecommunication Services Require Clearer Taxonomy and Legal Definitions

This section highlights how ecosystem definitions could be used interchangeably with the following section providing insight on how clarity around taxonomy could help with more structured classification.

4.1.1 Telecommunication Services

Section 2 of the bill defines telecommunication services broadly by including a wide variety of heterogeneous and possibly incongruous models. Many key terms, such as internet-based communication services, interpersonal communications services, and over-the-top (OTT) communication services are currently categorized collectively. The definitions could cause confusion around how services can be regulated.

Research suggests that the inclusion of the OTT communication services has been an issue of concern due to sparse definition expansion and a lack of a nuanced understanding of different models[56]. This could be further complicated with the emergence of multi-play entities as identified by the TRAI consultation paper released in January 2023 around converging models.

4.1.2 Interpersonal Communication

The term interpersonal communications can apply to a wide net of model types. Though it has been left undefined in the bill, a general understanding implies possible regulation of instant messaging apps, email platforms, video and audio call platforms, internet-based services and so on in an unfair manner.

4.1.3 Internet-based Communication

Ecosystem stakeholders refer to a variety of definitions from the global telecom industry ecosystem. Currently, the inherent understanding is that platforms that provide communication services over the internet in the form of message, voice, and video are referred to as 'internet-based communication' services. This includes but is not limited to communication-based services such as WhatsApp and Skype, social media applications such as Instagram and LinkedIn, and emailing platforms[57] inciting further confusion over how to understand model types.

4.1.4 OTT Communication Services[58]

Though OTT communication services also lack a universal definition, an attempt has been made to define and categorize them globally. European regulators (Body of European Regulators for Electronic Communications or BEREC) attempt to distinguish OTT services into three types of electronic communications (ECs).[59] Perceptions around the classification of OTT services are left for entities to self-determine, and most entities that are not telecommunications hardware providers or telecommunications network providers classify themselves as OTT services. This could inhibit innovation for emerging forms of technology and currently unimagined model types.

[56] Aapti primary and secondary analysis consolidation
[57] Call Hippo
[58] BEREC Report on OTT services
[59] ibid

The EECCs attempt to classify service and model types

The EECC categorises **OTT services** based on service model type and the competitive market that they are part of.

OTT - 0	Services that qualify as ECs
OTT - 1	Services that do not qualify as ECS but could potentially compete with ECs
OTT - 2	Services that are not an ECs and do not compete with ECSs

The EECC categorises **interpersonal communications** based on the engagement mechanism they are part of.

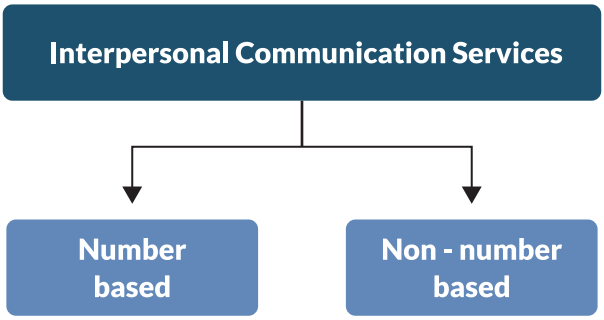


Figure 3: *Case study to understand attempts to classify by the EU*

4.2. The need for clearer definitions

With emerging business models, and with TRAI's nod to converging models, identification and clear mapping of models to regulatory bodies could prove to be challenging if not addressed at a functionality level. This could further increase challenges for the government in assigning jurisdiction and building capable regulatory bodies and could result in a variety of short- to long-term economic costs for both the government and business entities.

While a universal consensus on the classification structure is missing, a clear differentiation of network, infrastructure and subsequent digital layers would be the much needed starting point. A coherent taxonomy best suited to apply to the Indian jurisdiction, whether in the form of competing and non-competing OTT communication[60] services, significant and non-significant OTT communication services, or number-based[61] and number-independent electronic communications services[62], could prove to be starting points for classification.

With the emergence of bad actors in the ecosystem and a lack of transparency around how personal data is processed, regulation could be crucial in protecting users and entities within a digital economy, however basing regulation on unstructured model types could prove to be difficult. The following suggested framework offers a possible structured pathway to govern the various entities, beginning with creating structures based on three principles:

1

4.2.1 Differentiation between the layers

Differentiation starts at the layer. Telecommunications infrastructure provides the necessary configuration for networks to operate, which further gives rise to services that can be built 'on top of it'. Clearly differentiating between the layers could help provide a strong foundational difference between entity types.

2

4.2.2 Identification based on core services or features

Platforms can differ in the type of core service they are anchored on. While regulation needs

[60] BEREC Report on OTT services, BoR (16) 35
[61] Article 2(6), European Electronic Communications Code
[62] Article 2(7), European Electronic Communications Code

to be present to govern non-technical layers of such platforms, classification based on core service offerings could prove to be effective. With the convergence of various business features, secondary regulatory bodies could require expertise from various industries and sectors. However, identification of how these services operate could help reduce inefficiencies for relevant stakeholders.

Classification could be further based on various facets such as revenue size, user base, geographical presence. This could help determine how regulation, licensing and authorization could become more structured and allow for efficient innovation in and by the market.

3 **Identification based on resource being used**

Users can now access platforms through phone numbers or other unique identifiers such as email — spawning another layer where differentiation can be helpful.

5. Recommendations and Considerations

The internet was founded in the spirit of providing a boundaryless and unregulated data exchange infrastructure that would allow connections and efficient pathways across the globe. With countries creating and adopting future-ready frameworks, regulation plays a key role in improving user experience. The Indian Telecommunication Bill is a key element for progress in regulating the digital economy. However, further inquiry into the classification and licensing of various communication service models and a deeper unpacking of the costs and consequences could enable fair regulation, avert implications of over regulation, and sidestep what some experts call "over correction". In summation, the report makes the following recommendations for consideration:

5.1.1 Classification of entities by layer, and service type

A fundamental difference exists between these entities and the layer in which they exist and operate. Classifying telcos, OTTs, internet-based providers, and interpersonal communication services collectively may create friction and confusion when regulating different entities. Further exploration into classification of OTT service models need to be considered. The study suggests, identification and classification of entities based on:

Layer	Layer in which entities operate - e.g.: Telecommunication or Over-The-Top layer.
Core functionality	Communications based, or non-communications based. Further classifications could be structured around the competitive market that an entity operates in.
Mechanism of engagement	Number based, or non-number based. Entities could be differentiated on this parameter to improve regulatory mapping.

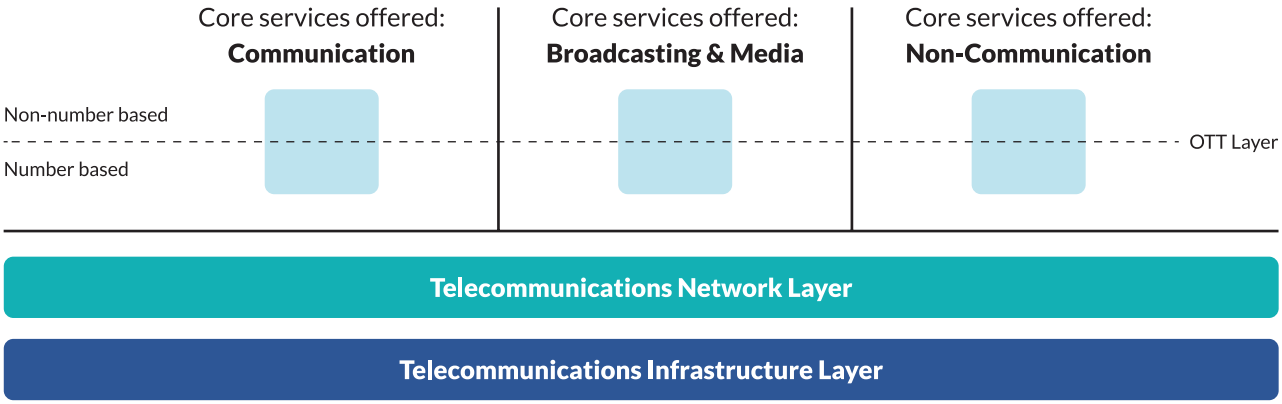


Figure 4: *Proposed framework to classify service models*

5.1.2 Finding minimum effective regulation, based on classification may be examined:

To ensure minimum effective regulation, particularly of smaller startups who face high barriers to entry, it may be valuable to provide exemptions to OTTs. Exemptions could manifest in the form of removing contributions to the TDF, contributions to network usage costs in addition to contributions to utilize the network for data and so on. While regulators can retain the powers of audit, consequences which increase the friction for users (rights to privacy and anonymity, access and affordability of information and communications technology) and newer startups needs to be addressed.

In this area, understanding regulatory capacity, especially among multi-play entities, could result in stronger and strategic governance mechanisms and allow for regulators to build effective capacity in the short to medium term.

5.1.3 Considering adjacent and supportive practices of data management to balance national security, while protecting secure communications

Documenting a clear framework when activating national security responses with a roadmap for permissions required and roles of officials clearly articulated could help address initial privacy concerns. Further, improving transparency around utilization of USOF/TDF and dedicating the allocated resources to improving access for underserved areas would be important. Additionally, creation of risk mitigation practices around data storage (from verification and other areas) — to reduce the risk of creating honeypots — could be adopted as industry standards. Platforms already deploy scrambling of plain text through encryption protocols to protect user privacy — storing of this encrypted data within acceptable time limits should also be considered.

5.1.4 Enhancing collaboration between the private and public sectors

Cooperation and collective effort are required from both sides to ensure the best service provision for users. This can be achieved by creating a more structured approach towards regulation (including collaboratively classifying and exploring implementation practice), collaborating on skill-sharing, and engaging directly with building users' literacy. To engage with users, increasing transparency and enhancing awareness, reducing friction around user verification, and championing initiatives and campaigns that work towards improving awareness and equity for users is the suggested way forward.

5. Appendix

Research methodology

The team conducted a secondary and primary research study to identify and articulate the findings shared above. Interactions took place with 10 industry and legal experts, reputed researchers, and academicians, from various organizations. The team leveraged robust desk research to inform the study — allowing for better triangulation of insights and information.

Key expert interactions

The study acknowledges and thanks the experts who shared their perspectives with the team via a semi-structured format. It is to be noted that the views of the respondents do not represent the views of the organizations they are a part of, and insights were aggregated based on the information collection mechanism used by the researchers.

Amrita Choudhury *CCAOI*	**Mansi Kedia** *ICRIER*	**Pranav Tiwari** *Internet Society*
Vertika Misra *NASSCOM*	**Dr V Sridhar** *IIIT - Bangalore*	**Neeti Biyani** *Internet Society*
Sunil Kumar Gupta *Independent Consultant*	**Vijayant Singh** *Ikigai Law*	**Mahesh Uppal** *ComFirst*
Nikhil Narendran *Trilegal, TMT*		

Ethical practices followed by the team:

- All secondary research has been sourced and attributed.
- Information from secondary sources has been consolidated and triangulated with information provided during the primary research phase of this study.
- Verbal and written consent for participating in the study has been collected for all respondents.
- Information collected during the primary research phase has been documented for the purpose of this study alone and will not be shared with external parties.
- Information collected during the primary research phase can only be accessed by the relevant members of the research team.
- Information for the primary research phase has been collected via notetaking during interactions. Any recordings of the interaction will be deleted after the conclusion of the study.
- Any comments or grievances around captured information can be shared with members of the research team at contact@aapti.in.

aapti institute 2023

Aapti is a public research institute that works at the intersection of technology and society. It examines the ways in which people interact and negotiate with technology both offline and online.

contact@aapti.in

aapti.in