The Dialogue™
INFORM ENGAGE IDEATE

Response

COMMENTS ON DRAFT INDIAN TELECOMMUNICATION BILL, 2022

Authors: Ayush Tripathi, Kamesh Shekar, Bhavya Birla and Eshani Vaidya
Edited By: Kazim Rizvi, Sreyan Chatterjee

The Dialogue™

INFORM ENGAGE IDEATE

Comments on Draft Indian Telecommunication Bill, 2022

Authors: Ayush Tripathi[1], Kamesh Shekar[2], Bhavya Birla[3] and Eshani Vaidya[4]

Edited By: Kazim Rizvi, Sreyan Chatterjee

[1] Ayush Tripathi is a Programme Manager - E-commerce, Payments and Telecom Vertical at The Dialogue.
[2] Kamesh Shekar is a Programme Manager - Privacy and Data Governance Vertical at The Dialogue.
[3] Bhavya Birla is a Research Associate at The Dialogue.
[4] Eshani Vaidya is a Senior Research Associate at The Dialogue.

ACKNOWLEDGEMENT

The research team would like to express our sincere gratitude to the participants of our focus group discussions for offering us their time and resources in collecting inputs for the response. We conducted a series of Focus Group Discussions with key stakeholders in the digital ecosystem. We obtained extensive inputs from 20 stakeholders with diverse backgrounds including academia, industry and civil society organisations. These inputs have helped us immensely to build our response on the Draft Indian Telecommunication Bill, 2022.

The Dialogue™
INFORM ENGAGE IDEATE

TABLE OF CONTENTS

I. Executive Summary

The Draft Indian Telecommunication Bill, 2022 (Draft Bill) aims to consolidate the current regulations into a singular framework. This proposed legislation would replace the Indian Telegraph Act 1885, Wireless Telegraphy Act 1933 and the Telegraph Wires (Unlawful Possession) Act, 1950. The bill introduces major reforms in the telecom sector. Provisions relating to providing relief to the entities in case of default payments, creating a regulatory sandbox, simplifying the framework for mergers and acquisitions, and providing clarity for operations during insolvency proceedings will immensely help the telecom industry. The added objective of the Telecommunication Development Fund to focus on R&D and skill development would spur growth and innovation in this sector. However, certain concerns in the Draft Bill need to be highlighted. Following are some of the issues that the Department of Telecommunications could look into:

Broad Definitions and Excluding Internet-based services from Telecom Bill

The definition of "telecommunication services" is very broad and covers a wide range of internet-based services that may or may not be the intention of the legislation. This definition could cover *any* internet-based service that uses communication as one of its tools. It needs to be kept in mind that the Draft Bill does not define any of the terms (such as internet-based communication services, interpersonal communication services, OTT (Over-the-Top) Communication services) mentioned under the definition of telecommunication services. This would lead to regulatory arbitrage, and a lack of understanding regarding the extent of coverage of this legislation.

In addition to the fundamentally distinct nature of telecom and internet-based services on the structural, technical and functional levels, another important reason not to include internet-based services in the draft bill is that they are already regulated by the Information Technology Act, 2000 (IT Act). Under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021(IT Rules), Internet-based services are subject to dedicated compliance and reporting requirements. Further, broadcasting services are covered by the Ministry of Information and Broadcasting ('MIB'). Regulating it under the draft bill would lead to jurisdictional overlaps.

Licensing Regime for Internet-based Services

Introducing a licensing regime as envisaged under the draft bill will increase barriers to entry, and impact innovation and the growth of the start-up ecosystem as compliance costs would increase significantly. A licensing regime fails to account for the fact that OTT services are often subject to rapid and evolving technological developments. Such a regime can adversely impact the internet-based services industry as their inherent nature and growth are systemically

intertwined with incorporating cutting-edge technological advancements to sustain their business. Further, such a licensing regime also would affect digital communities and would have a detrimental effect on data markets.

Interception of Messages

The draft bill replicates the power to intercept messages given under Section 5 of the Indian Telegraph Act 1885. However, with the expanded scope of telecommunication services, it would also include communications done through OTT communication service platforms. This increases the power of the authorities without putting in place any checks and balances for issuing the directive. It is also important to note that it covers encrypted messaging services. In the absence of a data protection bill, it may infringe on the individual's privacy rights. The bill presents an opportune moment to develop a comprehensive interception law that puts in appropriate safeguards and adheres to the necessity and proportionality tests laid down in Puttaswamy Judgement.

Further, another consequence of the expanded scope is that it will now cover the services that provide end-to-end encryption services. Entities providing these services might have to weaken their system to comply with the orders of interception. It also needs to be kept in mind that platforms providing end-to-end encryption services do not store data with them. In order to comply with the provisions, they will have to start storing such data, which will defeat the purpose of the end-to-end encryption service itself. The Telecom Regulatory Authority of India (TRAI), in its 2020 recommendations to DoT, had opined that the security architecture of end-to-end encrypted services should not be tinkered with as this will compromise the privacy, safety and security of citizens.

Dilution of Power of TRAI

The draft bill diluted the powers of the Telecom Regulatory Authority of India (‘TRAI’)and removed the parts wherein the government had to take recommendations from the authority before issuing licences, along with removing the currently existing prohibition on appointing government officials as chairpersons below the rank of secretary and additional secretary. These changes would impact the autonomy and functioning of the TRAI and dilute the collective decision-making power and knowledge transfer between TRAI and DoT.

Offences and Penalties

The bill provides excessive penalties for users of unlicensed services, which does not seem to be proportionate. Further, Imposing criminal liability on entities in a civil matter is excessive; instead, punitive action could be appropriate and proportionate to hold the entities accountable for any offence.

II. Clause by Clause Response

Clause	Our response	Recommendation
	Definitions	
Clause 2(18)	The spirit of the telecommunication law is to ensure a robust telecommunication network that delivers telecommunication services to users. Currently, the broad definition of telecommunication equipment may also include equipment not used to deliver telecom service.	- Telecommunication Equipment not used for user connectivity nor used to deliver the telecommunication service should not be considered telecommunication equipment.
Clause 2(21)	The definition of telecommunication services under the Draft Bill is very broad. Under the current definition, the bill would include all the internet-based services, which may not be the intention of the Draft Bill. Internet-based services should not be regulated under the telecom bill as these two are fundamentally different services in structural, technical, and functional aspects and are not substitutable. Further, regulating OTT under the telecom bill would lead to regulatory arbitrage and overlap with the IT Act, which regulates internet-based services. Further, it would lead to an excessive compliance burden on the entities, leading to a detrimental impact on startups.	- The bill must take cognizance of the technical and functional differences between TSPs (Telecom Service Providers) and OTT services. - The definition of telecommunication services should be limited to only services which operate in the network layer and should not include services in the application layer. - Jurisdictions such as the US, UK, EU, Canada, and Singapore also does not regulate OTT and Telecom services under an umbrella regulation. Therefore, India should not become a global outlier in this regard.

Licensing, Registration, Authorisation and Assignment		
Clause 4(1) & 4(2)	A licensing regime for OTT communication service providers will stifle the growth of existing services proposed to be brought under the ambit of "telecommunication services", and will also increase entry barriers for new players and impact the growth curve of an emerging sector.	- Re-consider the implementation of a licensing regime for OTT players, as it will stifle growth and innovation in the industry. - Reduce regulatory burdens on TSPs in line with ITU recommendations in favour of levelling the playing field with OTT players.
Clause 4(7)	Verifying an individual's identity or providing an identity for a natural person in digital space could become murky due to the existence of bots, deep fakes, manipulation, imposters, etc., leading to identity theft.	- The differentiation between anonymised and non-anonymised communication must be made clear within the bill to ensure that anonymous conversations are exempted from the purview of clause 4(7) & clause 4(8). - User identification information to be prescribed by the government has to be an additional way to identify the other users while the existing systems followed by various types of telecommunication services exist.
Clause 4(8)	This clause would hamper the anonymised conversation between two users enabled by internet-based communication services, which would, in turn, hamper freedom of expression.	
Spectrum Management		
Clause 5 (2)	In its current format, The Central Government plays the role of regulator, operator (through MTNL and BSNL) and licensor through administrative allocation. It is necessary that these clauses be amended in order to balance the playing field with private telecommunications operators.	- Cement auction of the spectrum as a primary mode of spectrum allocation due to its price discovery role. - Re-visit the expanded role and powers allocated to the central government in the interest of player parity in the industry.

Clause 5(2)(b)	Administrative allocation of spectrum, while backed with good intentions, needs procedural safeguards in order to ensure the neutrality of the regulator.	- Include procedural safeguards in the administrative allocation of spectrum.
Right of Way for Telecommunication Infrastructure		
Clause 17	The Bill paves the way for developing decentralised networks with a public interest motive at the forefront. Physical infrastructure forms a critical layer of enabling access to *any* digital service and must be given its due.	- Existing infrastructure should be leveraged, such as telecommunication infrastructure laid down by private entities. - Policies for digital public goods must ensure that physical infrastructure is given equal impetus. - The scope of open access and the relevant parameters for telecommunication law must be clearly defined (rules, FAQs and model contracting terms).
Standards, Public Safety and National Security		
Clause 24(2)	There is less clarity with the draft bill in terms of who would be a competent authority for interception approval, whether there will be a review committee etc.	- The new law must provide for setting up a Multi-Party Parliamentary Standing Committee to oversee the operations of law enforcement agencies and intelligence agencies. In addition, the parliamentarians must be granted access to information on intelligence and law enforcement agencies' operation and procurement, and a judicial oversight and review committee should be established. - The new law should have provisions for judicial authorisation for (a) prevention

		and investigation of criminal offences and (b) a special authority (to be created) for intelligence purposes that can be on the lines of the UK Investigative Powers Commissioner. - The existing review committee model formed under Rule 419A of the Indian Telegraph Act must be revamped in the new legislation representation of external members and experts. The constituted authority should be answerable to the Parliamentary Committee and the Parliament in general.
Clause 24(2)(a)	The new definition of "telecommunication services" would allow state actors to intercept information transmitted by messaging service providers, voice-over-IP service providers, video telephony software programs etc., which are traditionally encrypted to secure individuals' privacy. This provision would affect communication businesses, especially start-ups that innovate privacy safeguards and privacy-preserving technology and have consumer protection as an integral part of their business model.	- The draft Indian Telecommunications Bill must clarify how interception provisions would imply over businesses that traditionally don't hold any communication records. - The definition of "telecommunication services" is to be considered to ensure that some of the legacy encrypted services are exempted from the interception mandates
Clause 24(4)	While the procedures limit the duration of the interception, record keeping and usage of intercepted information, it doesn't limit the amount of data that can be accessed through surveillance. Due to no limitations, the agencies can retrieve data for a lifetime,	- Various technical safeguards must be established to protect the privacy of individuals following some of the below universal data protection principles like data

	i.e., from the day an individual uses a phone or internet service without any purpose.	minimisation, proportionality, purpose limitation etc. - The new law must ensure that every law enforcement agency and intelligence agency must have privacy/ethics officers within their agencies to ensure day-to-day operations are not violating privacy norms.
Telecommunication Development Fund (TDF)		
Clause 27	The expanded scope of the TDF, as proposed in the draft bill, is a much-needed intervention. The fund, as proposed, can be channelised towards increasing access to telecommunications services in uncovered areas, increasing the quality of services across the country. The fund's reliance on government initiatives needs to be revisited as they have not borne the fruits which were projected. Collaborating with private players in this domain thus will rejuvenate the fund's initiatives towards a more efficient course.	- Enable collaboration between stakeholders to maintain and revamp telecommunications infrastructure across the country. - Encourage private players to partake in the fund's primary objectives of enabling innovation, funding new technologies and increasing network coverage area.
Miscellaneous		
Clause 46	Clause 46 seeks to amend certain provisions of the TRAI Act, 1997. In the present form, it dilutes the power of TRAI with regard to recommending the central government on the issuance of new licences. This will have an impact on the function of TRAI as an independent body. It is important that DoT and TRAI work together to enable growth and innovation in the market. The to-and-fro between the two governing bodies is important to ensure checks and balances.	- It is recommended that clauses 46(d), 46(f), 46(g), 46(h) and 46(i) shall be removed from the draft bill.
Offences		

Clause 47	The draft bill provides a penalty for the users of unlicensed telecommunication services, which is alarming and should not be an offence. The ground for such a penalty is also vague and ambiguous and might lead to misuse. Further, it also provides criminal, and civil liability against entities found violating the bill. The criminal liability would be excessive, while civil liability could be proportionate. However, in case of continued violation even after notices, criminal liability may be proposed.	- Remove penal actions on the users of the telecom services - Remove criminal liability on the entities as it will impact innovation and growth of the ecosystem. - The power of search and seizure already exists under other laws, and there does not seem to be any rationale behind putting another provision in this bill.

III. Detailed Response on the Draft Indian Telecommunication Bill, 2022

1. Definition

Clause 2(21) of the Draft Bill defines telecommunication services as

"telecommunication services" means service of any description (including broadcasting services, electronic mail, voice mail, voice, video and data communication services, audiotex services, videotex services, fixed and mobile services, internet and broadband services, satellite-based communication services, internet-based communication services, in-flight and maritime connectivity services, interpersonal communications services, machine to machine communication services, over-the-top (OTT) communication services) which is made available to users by telecommunication and includes any other service that the Central Government may notify to be telecommunication services"

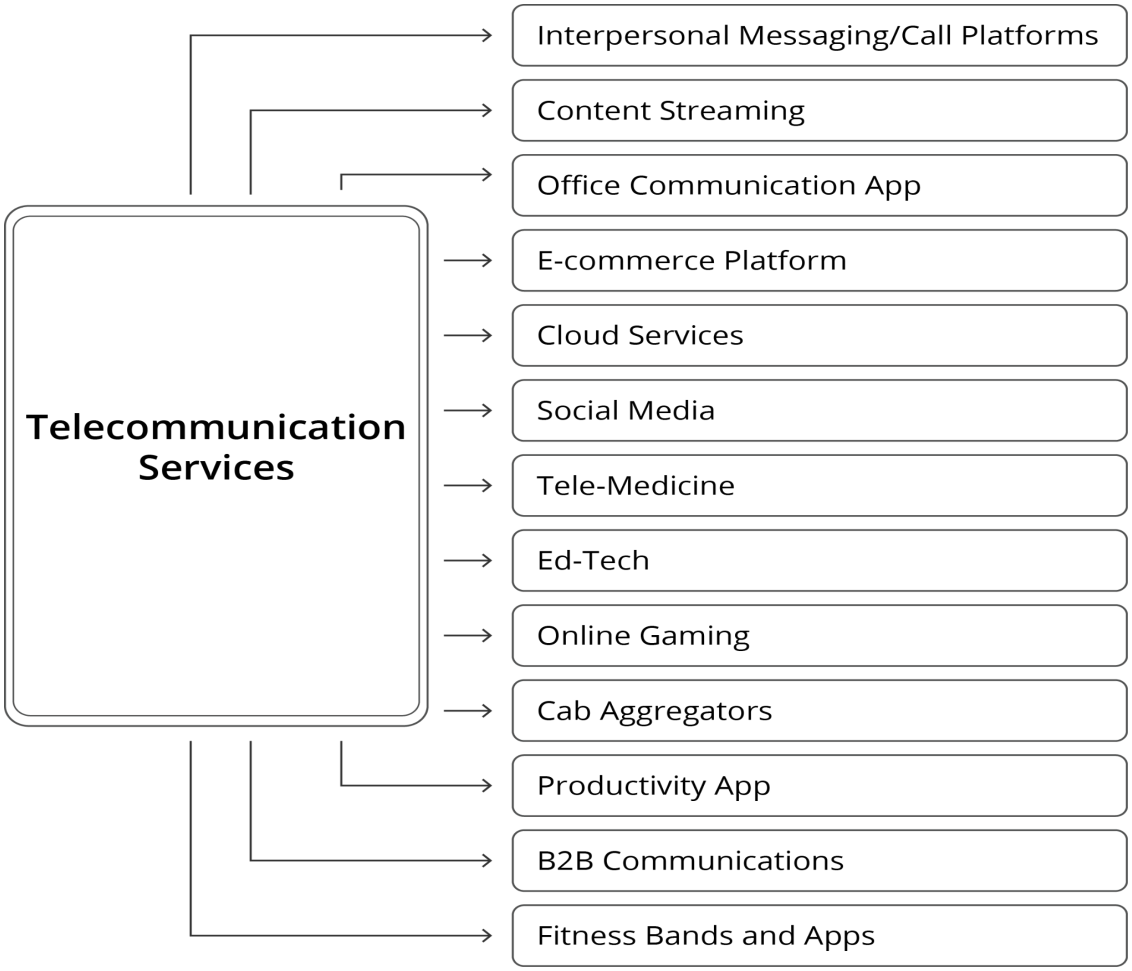
Prima facie, this definition is very broad and covers a wide range of services that may or may not be the intention of the legislation. Any internet-based communication app could be covered under this broad definition. It needs to be kept in mind that the draft bill does not define any of the terms mentioned in clause 2(21), which will create ambiguity and overlap with regard to the covered services. More specifically, the draft Bill does not define the term "over-the-top" ("OTT") communication services. Theoretically, OTT services can include all online services such as OTT communication, OTT media, e-commerce platforms, Internet Cloud Services, social media, web content, online gaming etc. **The overbroad definition will lead to regulatory arbitrage, and a lack of understanding regarding the extent of coverage of this legislation.**

Further, reading the definitions of 'messages' and 'telecommunication' together may be interpreted broadly to include all messages using telecommunication. For instance, notification messages within an app (i.e., in-app notifications/pop-up notifications) should not be treated/excluded from the scope of 'specified message' defined under clause 33 of the draft bill. As the term 'specified messages' is broadly worded, it is possible that such communications could include internal app-based notifications.

Services Covered under the Draft Bill

As mentioned above, the bill's definition covers a wide range of services which may not be the government's intention. Further, the draft bill does not define any of the terms mentioned in clause 2(21), **specifically OTT communication service,** as that would include a wide range of services.

Fig.1: **Business models covered under the definition of Telecommunication Services**



The consequence of such a broad definition would be that all of the services mentioned above would now have to obtain licences to operate in the country, that would mean another compliance burden in the long list.

While the definition is broad, a case is also made out that internet-based services and telecom services cannot be regulated under one umbrella law. Apart from the fundamentally distinct nature of these two services, which will be discussed in detail in the next section, another important reason for recommending the exclusion of internet-based services from the ambit of the draft bill is that they are already regulated by Information Technology Act, 2000 (IT Act). Under the Information Technology(Intermediary Guidelines and Digital Media Ethics Code) Rules 2021(IT Rules), internet-based services are subject to dedicated compliance and reporting requirements. **Another regulation on similar subject matter from different government departments would lead to regulatory arbitrage and overlapping jurisdiction.** The introduction of a licensing regime may qualify as an act of over-regulation on internet services

and not only increase compliance but introduce a crippling financial burden. This could hamper innovation and consumer choice and le.

Recommendations:

- There is a need for clear definitions and express carve-outs for the services that will not be governed by the framework.
- Internet-based services should not be regulated under telecom legislation.
- If any provision is required for the adherence of the internet services, it should be brought by MeitY under the IT Act, which is a more appropriate channel for internet regulation.

2. Case for distinct regulation of telecom and OTT services

The rationale behind the regulations put in place for the spectrum through TSPs and other licensing requirements are based on economic grounds as well as the scarcity of spectrum as a resource. Thus, ensuring a fair allocation of scarce resources; and, preventing any social harm that may arise from their misuse in the form of private benefit are the primary grounds for spectrum regulation. The Supreme Court of India has, over a long period of time, across judgments such as the *Ministry of Information and Broadcasting v Cricket Association of Bengal and Ors (1995)*[5], *Centre for Public Interest Litigation and Ors. v Union of India (2012)*[6] and *Bharti Airtel v Union of India (2015)*[7] maintained that spectrum is a valuable and scarce resource that degrades when not used efficiently. For these reasons, a licensing regime is implemented in spectrum allocation as it enables the government to monitor the usage of spectrum and intervene when necessary.

Article 39(b) of the Indian Constitution provides that the State needs to direct its policy towards ensuring the ownership and control of the material resources of the community are distributed to subserve the common good. In the context of telecommunications, the 'material resources' of the community are the spectrum and associated services that enable the distribution of this resource, such as internet and broadband services. However, services that run at the application layers over these distribution services, such as internet-based services, cannot be considered as a resource or service which is owned and controlled by the Central Government or that the Central Government has exclusive privileges over, because, in essence, these do not constitute natural resource but are services which are provided utilising the services that distribute spectrum. It also needs to be kept in mind that one of the regulatory principles is that the government should

[5] *Ministry of Information and Broadcasting v Cricket Association of Bengal and Ors* (1995) Retrieved October 12, 2022, from https://indiankanoon.org/doc/539407/
[6] *Centre for Public Interest Litigation and Ors. v Union of India* (2012). Retrieved October 12, 2022, from https://indiankanoon.org/doc/70191862/
[7] *Bharti Airtel v Union of India* (2015). Retrieved October 12, 2022, from https://indiankanoon.org/doc/36704852/

intervene only when there is a market failure. While spectrum is a natural resource, internet services which work on the application layer are not because (a) there is no scarcity because it is to an extent non-rivalrous, (b) there is the market where private players are already competing at the application layers.

Same Service same Rules Argument is not Applicable

Often, the argument of "same service, same rules" has been raised, claiming that there is a lack of a level playing field between telecom and OTT communication services as the OTTs are not subjected to similar amounts of regulation even though their services are similar to that of telecom. **There does not seem to be any merit to this argument, as these two services are not substitutable.** Telecommunications services and services based on internet protocols are so different that they could barely be considered competing "substitutes." For example, in the case of SMS vs internet messaging apps, it must be noted that the business models of these two services are different (consumption v. service/advertisement); their technology is different; the barrier of entry to the market is different, and their degree of availability to the public is different. For example - there are messaging platforms that are open for everyone to use, while others are closed or exclusive. Not having access to one of them does not imply endangering the right to communication, while not having access to SMS leaves the user with no available substitutes. **Services provided by OTTs are heavily dependent on data and voice services that are offered by the TSPs. Therefore, while TSPs can exist without OTTs, it is not possible for OTT services to be provided in the absence of TSPs.** As enumerated below, there is an inherent structural, technical and functional difference between the two services.

2.1 Structural and Technical Differences between Telecom and OTT Services

OTT service providers and TSPs function on a fundamentally different technical foundation. Communication data through OTTs is delivered in the form of data packets based on the best-effort delivery model, with no dedicated end-to-end channel being established for the duration of the communication. This starkly contrasts traditional voice services offered by TSPs, which function atop circuit-switched PSTN architectures, where dedicated communication channels are established between devices for the duration of the communication.[8] Digital Platforms and Services deliver Instant messaging data over IP networks as opposed to traditional SMS services, which utilise dedicated infrastructures involving short message centres, Short message entities and SMS gateways. At the same time, most TSPs already provide online

[8] Ikigai Law (2019 August 6) *'Over-The-Top' And 'Telecom' Services – Similar Or Not? - Our Analysis Of Stakeholders' Responses To Trai Consultation Paper.* Retrieved November 15, 2022, from https://www.ikigailaw.com/wp-content/uploads/2019/08/Final_Blog_OTT-services_060819.pdf *See also* Our Submission to TRAI's "Consultation Paper on Regulatory Framework for OverThe-Top (OTT) Communication Services" at https://www.trai.gov.in/sites/default/files/TheDialogue08012019.pdf

services and network access. Therefore, while TSPs can operate in network and application layers, internet companies are restricted to only the application layer.

In the Open Systems Interconnection (OSI) seven-layer model, a model used to standardise the functions of telecommunication and computing systems around the world, all seven layers work in tandem with one another to deliver content over the internet. Layer 3 works atop Layer 2, which works atop Layer 1 and so on.[9] OTT service providers function only on Layers 7 and 6, while the other layers are controlled by TSPs and Internet Service Providers (ISPs). In the case of OTT service providers, bits are transferred over various mediums, cables, ports, etc. Frames are used to define the data between two nodes on a data link, and when there are more than two nodes, the network helps address route and control traffic. The OSI model is a simple way to understand the hierarchy of layers, where layer 3 works with IP addresses, and layer 2 works with MAC addresses. For example, a house address is always the same, like a MAC address, while an IP address can change, like the addressee at the house.

Much like the difference between Layer 3 and Layer 2 in the OSI model, the routing function is the main difference between a Layer 2 switch and a Layer 3 switch. A Layer 2 switch only works with MAC addresses and doesn't interact with any higher layer addresses, such as an IP. A Layer 3 switch, on the other hand, can also do static and dynamic routing, including IP and virtual local area network (VLAN) communications. This dual-layer functionality is why a Layer 3 switch is also known as a multilayer switch.[10]

OTT service providers only cover the topmost layers, while control over the rest is in the hands of the TSP or ISP, highlighting how little control or decision-making power OTT service providers have over the ecosystem. In such a model, TSPs and ISPs have adequate powers to control data prices, service areas, and service offerings, all within the ambit of net neutrality that can have a tangible impact on OTT service providers.

Additionally, OTT service providers do not make use of the scarce public resource that is Spectrum and do not provide access to a network, so the need for a licensing regime does not arise. As regards the quality of service, OTTs cannot deliver their services independently of the network provided by TSPs. It is TSPs which act as gatekeepers of the internet, and the quality of service delivered by an OTT platform depends most often on the quality of the underlying network.[11]

---

[9]O'Keeffe, A. (2022, May 16) *OSI layers: Everything you need to know*, Aussie Broadband. Retrieved October 13, 2022, from https://www.aussiebroadband.com.au/blog/osi-layers-everything-you-need-to-know/

[10]O'Keeffe, A. (2018, October 20)) *The difference between Layer 3 and Layer 2 networks*, Aussie Broadband. Retrieved October 13, 2022, from https://www.aussiebroadband.com.au/blog/difference-layer-3-layer-2-networks/#:~:text=A%20Layer%202%20switch%20only,area%20network%20(VLAN)%20communications.

[11]Asia Internet Coalition(2018, December 28) *Submission on the Consultation Paper on Regulatory Framework for Over-The-Top (OTT) Communication Services in India.* Retrieved October 13, 2022, from

The Telecom Regulatory Authority of India has, in its recommendations on the Regulatory Framework for Internet Telephony in 2017 ("Internet Telephony Recommendations"), also emphasised that the separation of network and service layers of telecom service offerings is the natural progression of the technological changes in this domain.

The same trend needs to be reflected in the regulations for such networks and service layers for OTT communication service providers. Subjecting new-age OTT service providers to traditional regulatory regimes will only have the impact of creating huge entry barriers, as opposed to supporting innovation and development. Therefore, the question should be limited to whether there is parity in the treatment of TSPS and OTT communication service providers only to the extent of services provided by them.[12]

These technical differences prove that OTT service providers are not substitutes for TSPs and the traditional telecommunications infrastructure. OTT service providers rely on TSPs to drive data consumption and increase revenues. This can be easily understood through an assertion: OTTs need stable internet access. If such access is disrupted, the OTT platform ceases to work, establishing the existential reliance of OTT service providers on infrastructure controlled and maintained by TSPs. For these reasons, we believe that OTT service providers complement TSPs, not supplant them.

2.2 Functional Differences

Services offered by OTTs and TSPs are distinct in nature. While there is overlap in the communication services like calling and instant messaging, OTT service providers add multiple utility functions such as sharing files, media, taking polls, and in certain 'super apps', multiple services, typically out of the domain of an OTT communications services provider are also bundled. The bundling of services that differentiate OTT service providers from traditional TSPs is a fundamental milestone for OTT service providers, as bundling of features is an important step in the organic progression of any OTT service provider.

Often, the settled assertion of 'same service, same rules' is presented by the TSPs, claiming that the functional overlap has led to OTT applications taking over the voice revenue of TSPs due to the price arbitrage between voice tariffs and equivalent data tariffs for voice calls over the Internet. But this argument of loss of revenue lost its relevance when a new TSP made voice calling free/as part of bundled data packs. In the present scenario, it is important to note that the market itself has shifted in a direction where voice revenues are no longer relevant. With the new

https://trai.gov.in/sites/default/files/AsiaInternetCoalition08012019.pdf

[12]TRAI (2017, October 24) *Recommendations On Regulatory framework for Internet Telephony.* Retrieved October 15, 2022, from https://trai.gov.in/sites/default/files/Recommendations_24_10_2017_0.pdf

tariff plans released by new entrants and incumbents, the TSPs are shifting to a data-only model with unlimited voice calls.[13]

Referring to OTT and conventional telecom as the "same service" is flawed. Telecom operators control the underlying broadband access infrastructure and are the gatekeepers to broadband internet access, as discussed above.

To suggest that there is a natural parity or similarity between OTT players and Telecom Service Providers (TSPs) is also erroneous. The latter enjoy several exclusive rights conferred on them through their licences not enjoyed by online services, such as the right to acquire spectrum, the right to obtain numbering resources, the right to interconnect with the PSTN, and the right of way to set up infrastructure. On the other hand, no exclusive privilege is granted to OTT players. Further, since there are no entry barriers for providing OTT services, even TSPs can enter the OTT market without an additional licence, whereas OTTs cannot enter the TSP market without a licence. While TSPs can operate in both the network and application layers, OTTs are restricted to the application layer and cannot enter the network layer.[14] OTT provides rich interactions beyond text and voice communication on the application layer, and that's the innovation which should not be curbed.

OTT communication services should not be seen as substitutes for traditional TSPs. Instead, they should be valued for the rich interaction they build through leveraging services like file, image and audio sharing on top of their communication services. It is these rich interactions that drive user engagement as they provide services that simplify day-to-day tasks such as file sharing and payments and, in turn, benefit the network layer as much as the application layer by driving greater data consumption.[15]

This is a distinction that arises not from service providers but from consumers themselves. Further, any distinction between OTT communication services and other OTT services is artificial, as most OTT services tend to develop platform characteristics that incorporate communication as only one aspect of the wider service provided. A good example of this progression can be seen in the development and subsequent adoption of Google's WebRTC API that enables messaging and communications services on any website.[16] As a result, asking for

[13]Joshi, S. et al. (2015 February) *Impact of Over the Top (OTT) Services on Telecom Service Providers*, Indian Journal of Science and Technology 8(S4):145. Retrieved October 13, 2022, from https://www.researchgate.net/publication/276175550_Impact_of_Over_the_Top_OTT_Services_on_Telecom_Service_Providers
[14]Broadband India Foundation (2017 April 27) *Counter Comments from BIF on TRAI consultation paper on Net Neutrality.* Retrieved October 13, 2022, from https://trai.gov.in/sites/default/files/BIF_27_04_17.pdf
[15]ITU-D Study Group (2021) *Economic impact of OTTs on national telecommunication/ICT markets.* Retrieved October 13, 2022, from https://www.itu.int/dms_pub/itu-d/oth/07/23/D07230000030001PDFE.pdf
[16] Google, *WebRTC*, Retrieved October 13, 2022, from https://webrtc.org/

regulatory parity on the basis of the "same service, same rules" argument is incorrect and does not justify a higher regulatory burden on Over-the-Top (OTT) players.

2.3. Regulations of Telecom and Internet services in other Jurisdictions

Since regulatory overlap between OTT service providers and TSPs is a global phenomenon, we can study international approaches to the issue in order to ascertain the necessary magnitude of the regulatory response to address overlaps.

2.3.1 International Telecommunications Union (ITU)

The International Telecommunications Union is the international regulatory body that aims to standardise telecommunications and internet laws globally to enable interoperability between jurisdictions and drive growth. The ITU has long been adjudicating the need for collaboration between OTT service providers and TSPs and has drafted broad recommendations to harmonise the telecommunications landscape globally. Towards this, the ITU has stressed the following solutions:-

- Collaboration between TSPs and OTTs is necessary at the National and International levels.[17]
- There is a need to reassess the magnitude of regulations on TSPs instead of increasing regulations on OTTs to bring about regulatory parity.[18]
- The future is data-centric, and thus, there is a need to undertake viability assessments of current voice and SMS-reliant business models in order to stay up to speed with increasing data consumption, technological advancements and evolving consumer needs.[19]
- The ITU has also recommended that OTTs be regulated under a framework that is cognisant of the technicalities of how such services are offered.[20]

In its 2019 recommendations titled 'Collaborative Framework for OTTs', drafted by the ITU-T Study group 3 tasked with overseeing and researching OTT platform regulations globally, the ITU recommends that government reduce regulatory burdens for TSPs instead of increasing regulations for OTTs in order to level the playing field.[21] The ITU-T Study Group 3 released another recommendation document titled 'Enabling environment for voluntary commercial

[17] ITU-T (2019 May 2) *Collaborative framework for OTTs.* Retrieved October 14, 2022, from https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13595
[18] ITU-T (2020 August 28) *Enabling environment for voluntary commercial arrangements between telecommunication network operators and OTT providers.* Retrieved October 14, 2022, from https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14269&lang=en
[19] *Ibid.*
[20] *Supra Note 16*
[21] *Supra Note 16*

arrangements between telecommunication network operators and OTT providers' in 2020, calling for TSPs to consider shifting their business models to become more data-centric as internet calling and data usage, were at an all-time high and have not since lowered. [22]

A 2020 annual deliverable report of the ITU-D Study group assessed the benefits of a collaboration between TSPs and OTT platforms, coming to the conclusion that such collaboration has resulted in benefits such as reduced churn rates, increased net promoter scores, more stable in-bundle revenue streams, and the ability to link returns more directly to network investment. The study also establishes that in a data-driven future, a collaboration between both parties is crucial for harmonious growth as both sides rely on one another for revenue making and can potentially complement one another. [23]

It is now evident that consumption of content through OTT platforms has significantly boosted revenues for TSPs globally.[24][25] The consumption trend also highlights that consumers are always interested in moving to a faster internet connection when available, as their content needs have cemented. Furthermore, in its 2021 publication titled *'Emerging technologies, including cloud computing, m-services and OTTs: Challenges and opportunities, economic and policy impact for developing countries'*, the ITU states that regulation of OTTs is not always required as mandating legacy requirements on emerging markets, can dampen innovation if not approached correctly. The document highlights global projects undertaken by OTTs in building infrastructure and improving networks in tandem with TSPs and ISPs to provide better services to consumers globally.[26]

Thus, the ITU recommends reducing regulatory burdens on TSPs and their business models and reimagining centre data usage in the coming years. OTT applications drive the demand for Internet connectivity services, thus increasing traffic and, consequently, the revenue of telecommunication service providers. Broadband services are usually offered with commercial models linked to data usage, involving transfer speed and traffic amount, typically tied to minimum consumption.

---

[22] ITU-T (2020 August 28) *Enabling environment for voluntary commercial arrangements between telecommunication network operators and OTT providers.* Retrieved October 14, 2022, from https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14269&lang=en

[23] *Ibid.*

[24] Dey, A. (2019 May 12) *OTT players ride piggyback on telcos to boost revenues*, Financial Express. Retrieved October 15, 2022, from https://www.financialexpress.com/life/technology-ott-players-netflix-hotstar-amazon-prime-video-zee5-ride-on-telcos-airtel-reliance-jio-vodafone-idea-to-boost-revenues-1575769/

[25] ITU-D Study Group 3 (2019 October 1) *Question 3/1 and 4/1 Joint session on the Economic impact of OTTs on National Telecommunication/ICT Markets.* Retrieevd October 15, 2022, from https://www.itu.int/dms_pub/itu-d/oth/07/1a/D071A0000040002PDFE.pdf

[26] ITU-D Study Group 3 (2021 February 3) *Emerging technologies, including cloud computing, m-services and OTTs: Challenges and opportunities, economic and policy impact for developing countries.* Retrieved October 15, 2022, from https://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.03.2-2021-PDF-E.pdf

The ITU also recommended member states create a conducive environment for agreements between OTT platforms and TSPs for infrastructure development and management to manage the ever-increasing internet adoption and digitisation of our lives.

2.3.2. United States of America (USA)

The Federal Communications Commission is the regulatory authority for telecommunications and internet services in the USA. The FCC has in the past adjudicated differences between OTT platforms and traditional TSPs over a level playing field and other regulatory clashes however has always concluded that there is no need to regulate OTT communications services similar to TSPs. However, it mandates data protection standards, emergency calling services and contributions to the Universal Services Fund and the Telecommunications Relay Services Fund at par with TSPs[27].

2.3.3. Canada

In February 2022, the Canadian government introduced a new bill to amend the Broadcasting Act and to make related and consequential amendments to other acts, such as the 'Online Streaming Act'. The Online Streaming Act aims to expand the authority and powers of the Canadian Radio-television and Telecommunications Commission (CRTC), and it will bring online broadcasters – including online streaming platforms – under the same regulatory framework as traditional broadcasters providing services and content in Canada[28].

Although the CRTC has recognised that new media digital and Internet content delivery platforms do fall within the definition of "broadcasting" for the purposes of the Broadcasting Act, it exempted these platforms from broadcast licensing and regulation through the promulgation of successive digital media exemption orders.

2.3.4. European Union (EU)

In the European Union, the European Electronic Communications Code, with its amendments in effect from December 2020, subsumed a host of new OTT services under its definition of 'electronic communications services', thereby mandating Data protection, compliance with law enforcement requests, emergency dialling services and consumer protection laws[29]. The

[27]Brown, A. & Trapp, D. (2021 August) *Telecoms & Media 2021*, Law Business Research. Retrieved October 19, 2022 from https://www.hwglaw.com/wp-content/uploads/2021/08/2021-Telecoms-Media.pdf
[28] Senate of Canada (2022 November 4) *The Online Streaming Act in the Senate*, Government of the Dominion of Canada. Retrieved October 20, 2022 from https://sencanada.ca/en/sencaplus/news/the-online-streaming-act-in-the-senate/#:~:text=The%20Senate%20is%20debating%20Government,regulator%2C%20among%20many%20other%20things.
[29]Parliament of the European Union (2018 December 11) Directive (EU) 2018/1972 *Establishing the European Electronic Communications Code*. Retrieved October 18, 2022 from

Technical standards with which OTT platforms in the EU must comply are outlined by the European Union Agency for Cybersecurity (ENISA) under their 'Guideline on Security Measures under the EECC'.[30]

The Body of European Regulators for Electronic Communication **(BEREC)** outlined the models in which OTT platforms function and their relative overlaps with traditional TSP services in order to ascertain which OTT platforms can be regulated similarly. BEREC has in the past also recognised the utility OTT platforms bring to TSPs and consumers, stating, *"ultimately, it is the success of the [content and application providers] […] which lies at the heart of the recent increases in demand for broadband access (i.e. for the ISPs' very own access service)"* This supports the view that without new and innovative online content and applications, the value of Internet access to users would be severely reduced.[31]

BEREC classifies OTT as

- **OTT0-** OTTs that qualify as Electronic Communication Services (ECS)
- **OTT1-** OTTs that do not qualify as ECS but compete with traditional TSP (e.g. Whatsapp)
- **OTT2-** OTTs that do not qualify as either (e-commerce, video and music streaming)[32]

The European Union, however, still doesn't mandate licensing models for OTT platforms in the manner envisaged under the draft bill. This is true for other progressive economies such as the United Kingdom and the United States of America as well.

2.3.5 Singapore

Singapore currently mandates licensing for OTT platforms and differentiates OTT communications services from traditional TSPs on the grounds of spectrum use. Essentially, to be regulated as a 'telecommunications service' under the country's Telecommunications Act of 1999[33]spectrum usage is required. Due to OTT communications services being internet-based,

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L1972&from=EN

[30]European Union Agency for Cybersecurity (2021 July 7) *Guideline on Security Measures under the EECC*. Retrieved October 18, 2022 from https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

[31]BEREC (2012 November 14) *BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines*. Retrieved October 18, 2022, from https://www.berec.europa.eu/en/document-categories/berec/others/berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines

[32]BEREC (2016 January) *Report on OTT Services*. Retrieved October 19, 2022, from https://www.berec.europa.eu/sites/default/files/files/document_register_store/2016/2/BoR_%2816%29_35_Report_on_OTT_services.pdf

[33] Ministry of Communications and Information (2021 December 1) *Amended Telecommunications Act, 1999,* Government of the Republic of Singapore. Retrieved October 25, 2022 from https://sso.agc.gov.sg/Act/TA1999

they are covered under the Broadcasting Act[34] instead. Their licensing regime for OTT television service providers grants automatic permission to applicants if they take the undertaking to comply with Singapore's Code of Conduct for Over-the-Top, Video-on-Demand and Niche Services[35], granting them a Services Based Operations (SBO) license as they operate on established telecommunications infrastructure[36], authorised by the industry regulator, Info-Communications Media Development Authority (IMDA). The SBO licence is closer to a registration formality as these licences are not required to be updated regularly under the current regulations. Instead, they are valid up until the IMDA rescinds the licence for any notified breach.[37]

Furthermore, OTT Platforms that cater to audio-visual content streaming make available their offerings to all users all at once in an asynchronous manner (any person can watch the video or audio content as per their choices), which is in stark contrast to the one-to-one communications that are synchronously enabled by TSPs (two users are often needed to communicate on call, text, video calls etc.). This is a primary ground of differences in the operations of the two sectors, signifying their separate uses. Thus, if India were to consider a stringent licensing regime for the applications layer, it would mark a significant departure from international best practices.

Recommendations:

- Owing to the fundamentally different nature of the telecom and Internet-based services, as discussed in detail above, it is recommended that these two services are not regulated together.
- India will become a global outlier if it attempts to regulate these two services together with the licensing regime.

[34] Ministry of Communications and Information (2021 December 1) *Amended Broadcasting Act, 1994,* Government of the Republic of Singapore. Retrieved October 25, 2022 from https://sso.agc.gov.sg/Act/BA1994
[35] IMDA, *Code of Conduct for Over-the-Top, Video-on-Demand and Niche Services*. Retrieved October 23, 2022 from https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/codes-of-practice-and-guidelines/acts-codes/ott-vod-niche-services-content-code-1mar2018.pdf
[36]Ministry of Communications and Information (2021 December 1) *Telecommunications (Class Licences) Regulations, 2011.* Government of the Republic of Singapore. Retrieved October 25, 2022 from https://sso.agc.gov.sg/SL/TA1999-RG3?DocDate=20161003&ProvIds=P1I-#pr1-
[37]Chong Kin, L. (2021 December 10) *Telecoms, Media and Internet Laws and Regulations Singapore 2022,* Drew & Napier LLC. Retrieved October 25, 2022 from https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/singapore

3. Licensing, Registration, Assignment and Authorisation

3.1. Licensing, Registration, Authorisation and Assignment of OTT and Internet-based Services

As mentioned above, the creation of a licensing regime for providers of OTT communication services has been a consistent demand of traditional telecom service providers. According to TSPs, the lack of equal or same regulations over OTT communication service providers creates an uneven playing field as OTT services are a "substitute" for their services. Additionally, TSPs also argue that the increasing use of OTT communication service providers by users has led them to suffer from loss of revenue due to loss of market share.

Clause 3(1) of the Bill provides the Union Government with the exclusive privilege to provide telecommunication services, establish & operate telecommunication networks and infrastructure, and use and allocate spectrum. In exercising this privilege, Clause 3(2) of the Bill allows the Union Government to prescribe licences for providing telecommunication services or establishing, operating, maintaining and expanding telecommunication networks. Further, Clause 4(1) states that this privilege will be provided through rules that the Union Government may prescribe at a later date for payment of entry fees, licence fees, registration fees or any other fees or charges. Thus, each service included in the list of services in the expanded definition of "telecommunication services" will now have to obtain a specific licence to operate in India.

A licensing regime fails to account for the fact that OTT services are often subject to rapid and evolving technological developments. Such a regime can adversely impact the internet-based services industry as their inherent nature and growth are systemically intertwined with incorporating cutting-edge technological advancements to sustain their business. A licensing regime will stifle the growth of existing services proposed to be brought under the ambit of "telecommunication services", and will undoubtedly increase entry barriers for new players and impact the growth curve of an emerging sector. The licensing regime would bring additional compliance burdens and associated costs, putting immense pressure on the startups. If a licensing regime is proposed for internet-based services, they will also have to pay an entry fee, periodic licence renewal charges and other costs. Any internet-based services also have to comply with the Information Technology Act and other sectoral laws, and adding another licence or registration process would raise entry barriers and significantly impact the ease of doing business. It needs to be kept in mind that the Indian government has recognised this sector as crucial for propelling India into the next phase of its growth.

Additionally, the Ministry of Information and Broadcasting (MIB) already carries out the licensing and regulation for broadcasting services. The imposition of another licensing regime and other compliance requirements for broadcasting services as proposed under the draft bill is

only likely to add additional burdens on providers, including increased financial obligations. This may negatively impact the growth of the broadcasting sector as it may require broadcasting services providers to redirect their investments from research and development into operation costs such as compliance requirements.

Case of Over and Excessive Regulation

OTT service providers are already subject to existing laws governing interception, privacy, cybersecurity, etc., including the IT Act and its rules (such as the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, CERT-In Directions 2022[38], and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021). They will also be subject to the compliance burden under upcoming data protection law and the possible Digital India Act that the Government considers a more rigorous replacement for the IT Act. Similarly, broadcasting services are already subject to various legislations such as the Cable Television Networks (Regulation) Act, 1995 and rules thereunder, administered by the MIB.

The requirement of a licence, approval or authorisation for the provision of internet-based communication services runs contrary to TRAI's observations in its recommendations on "Regulatory Framework for Over-The-Top (OTT) Communication Services".[39] TRAI observed that a comprehensive regulatory framework for OTT services is not recommended beyond the existing laws and regulations. It was of the opinion that such regulation could be looked into afresh when more clarity emerges in international jurisdictions. Bringing internet communication services within the regulatory ambit of DoT would not only subject such services to onerous licence terms and conditions but would also include a levy of entry fees, licence fees and registration fees. This will have a chilling effect on innovations and investments in the internet ecosystem.

Recommendations:

1. Excessive regulation would adversely affect a medium that has helped citizens to communicate securely. Licencing would change many open-source projects that help people communicate and exchange ideas securely. It is recommended that licensing and

[38] Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, issued by the Indian Computer Emergency Response Team dated April 28, 2022.
[39]TRAI (2018 November 12) *Consultation Paper On Regulatory Framework for Over-The-Top (OTT) communication Services.* Retrieved October 29, 2022, from https://www.trai.gov.in/sites/default/files/CPOTT12112018_0.pdf

registration of communication services should not be applicable to internet-based services.

3.2. Identification of Users

Clause 4(7) of the draft bill mandates the entities to identify the users of their platform through a verifiable mode of identification as may be prescribed. This may entail a KYC-like process where the entities can ask for government-issued identification cards. Additionally, clause 4(8) mandates the identification of the sender of a message that needs to be made available to the receiver. The rationale given in the explanatory note behind introducing such a provision is to prevent cyber fraud.

While the intention behind bringing this provision is good, these provisions dilute the individual right to privacy. This would start large-scale data collection and retention practices, that too in the absence of a data protection law. This provision also takes away the right to stay anonymous and would have a detrimental impact on the whistleblowers or employees who want to raise their concerns about the workplace anonymously

It is important to steer clear of a broad brush approach that mandates verifiability of *all* users of telecommunication networks. Not only would this conflict with the 'proportionality test' established by the Supreme Court[40], but the overcorrection will also do away with anonymity within the Internet Stack, which can have lasting and harmful consequences. While the need for verifiability is understandable to curb harms related to disinformation, misinformation, or even identifying those that publish Child Sexual Abuse Material ('CSAM'), a risk-based approach to verifiability must be adopted. For instance, one's medical information, as sensitive personal data, must remain anonymous. However, spreading false information about measures against COVID-19 must ensure that the publisher is clearly highlighted so as to determine credibility. A broad brush approach such as this will do away with a critical aspect of the internet, i.e. ability to bring a sense of 'community' into our digital lives. There is a need to explore verifiability as a flexible method of identity with various gradations for various types of services that helps to create a safe environment across online services.

Besides, as the users of telecommunication services identify other users through various means, for instance, using the telephone number, using profile name etc., additional standards to be prescribed by the government must be congruent to these systems to avoid reinventing the wheel again. Further, verifying an individual's identity as per clause 4(7) or providing an identity for a natural person in digital space could become murky due to the existence of bots, deep fakes, manipulation, imposters, etc., leading to identity theft.

[40] *Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors. (2017)*. Retrieved November 8, 2022, from https://indiankanoon.org/doc/127517806/

Recommendations:

1. Such large-scale data collection should not be allowed at this stage. It may be reconsidered after a data protection law is put in place along with providing additional safeguards.
2. The differentiation between anonymised and non-anonymised communication must be made clear within the bill to ensure that anonymous conversations are exempted from the purview of clause 4(7) & clause 4(8).
3. User identification information to be prescribed by the government has to be an additional way to identify the other users on top of the existing systems followed by various types of telecommunication services. A collaborative approach between telcos and communication services could be better here.

4. Right of Way for Telecommunication Infrastructure (Open Access under Clause 17 of Draft Bill)

Ensuring last-mile internet and telecom connectivity across the country requires a deeper look at the manner in which the foundational infrastructure is being built and maintained. One of the key building blocks is that of the common ducts or conduits, or cable corridors. Clause 17 grants the Central Government the power to establish such ducts in publicly financed infrastructure projects. The Clause also provides that the telecom infrastructure thus established must be granted to third-party facility providers on an open-access basis.

We would draw attention to further detail and clarify the meaning of this clause. Clause 17 is a stepping stone towards building decentralised networks that are governed by some public interest motivations alongside a profit motive. It allows for more affordable services, which can move up the stack, in addition to paving the way for improved last-mile service delivery. With a public-interest-driven initiative, the definition of connectivity and accessibility can also curb the growing instances of ring-fencing of digital and digital-enabling assets.[41] Access to telecom services also includes internet access at speeds that enable meaningful utilisation of the services. For instance, if under-connected areas constantly face issues like calls dropping or have trouble finding 'network coverage areas'[42], then the objective of increasing financial inclusion or setting the base for digitally enabled development will not be adequately met.

Open access and its parameters for the purpose of telecommunication law must be clearly defined - if needed through a combination of Rules, FAQs and model contracting terms. This will have a positive knock-on effect on initiatives like PM Gati Shakti that also rely on such connectivity and seek to improve the movement of goods, services and people across the

[41] Tarnoff, B. (2022). *Internet for the People: The Fight for Our Digital Future*. Verso.
[42] People in remote areas often receive 'out of network coverage' messages from their network provider.

country.[43] As expressed in the National Digital Communications Policy, it is important to 'leverage existing assets'.[44] This is also reflected in clauses 14(3)[45], 15[46] and 16[47] of the Draft Bill. Successfully leveraging digital public goods requires strong linkages with the infrastructural backbone of the concerned initiative. The aforementioned clauses are a reflection of the government's goal of creating a more inclusive telecommunications sector.

The next step could be establishing the link to digital public goods in these clauses. Within this context, increased coordination between Digital India initiatives or between those along open governance, will allow for the sharing of infrastructure. The Telecom Bill, 2022 must clearly enable linkages between public goods so that cutting-edge innovations in facilitating the growth of various digital markets (such as the Open Network for Digital Commerce or Kochi Smart Mobility Network) are actualised in a manner that covers both physical and digital telecommunications infrastructure, to promote digital public goods with a strong public interest incentive.

[43] National Portal of India. *PM Gati Shakti - National Master Plan for Multi-modal Connectivity*. Retrieved November 8, 2022, from https://www.india.gov.in/spotlight/pm-gati-shakti-national-master-plan-multi-modal-connectivity
[44] Clause 1.1 (b) (iv) of National Digital Communications Policy
[45] The Central Government has the authority to acquire a right of way to establish, operate and maintain telecommunication infrastructure.
[46] Non-discriminatory and non-exclusive grant of right of way.
[47] Telecommunication infrastructure distinct from the property on which it is installed.

5. Standards, Public Safety and National Security

The Telecom bill presents an opportune moment for the government to come up with a comprehensive surveillance regime which puts in appropriate safeguards and adheres to the mandates of *Puttaswamy Judgement.* However, the regulatory framework for interception proposed in the draft Indian Telecommunication Bill has significant gaps which need to be addressed. The draft bill provides discretionary powers to perform targeted interception of communications without appropriate checks and balances.

5.1. Definition

Across chapter 6 of the draft Indian Telecommunication Bill there has been a loose connotation to terminologies like public order, national security, public safety etc. However, these terms that set the boundaries for interception are not well defined and understood[48] and are open to wide interpretation and misuse. This is especially true for the term "National Security" (most used for targeted surveillance[49]), "public order", and "investigation" of a crime. Also, overarchingly, India lacks a national security strategy that could clarify the definition of national security and the objective of ordering interception.

This lack of understanding and clear boundaries of "national security", "Public Emergency", etc. within the bill is concerning. For instance, clause 24(4) of the draft bill provides that interception shall be continued until a public emergency exists or the interests of public safety require the same. However, we do not know what situations would be perceived as a threat to "national security" and "Public Emergency", leading to unintended consequences like false positives etc. Moreover, this would also leave room for expansive interpretations and, thus, facilitate unintended surveillance of personal and private communications.

Recommendations:

1. There is a need to move from the broad language used in the status quo to defining critical terminologies such as national security, public order etc. and principles like proportionality, necessity, suitability, and legality, etc.

[48] Shekar, K., & Mehta, S. (2022, February 17). *The state of surveillance in India: National security at the cost of privacy?*. ORF. Retrieved March 12, 2022, from https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/
[49] Sirohi, N. (2021, August 7). *Pegasus in the Room: Law of surveillance and national security's alibi*. ORF. Retrieved March 12, 2022, from https://www.orfonline.org/expert-speak/pegasus-in-the-room-law-of-surveillance-and-national-securitys-alibi/

2. The definitions must be specific and must expressly clarify the rights and corresponding duties as to avoid the creation of any loopholes.[50]

5.2. Lack of Clarity in Interception Authorisation

Under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, no agency or person can perform interception without the direction and approval of the competent authority. The competent authority under the rules is the Home Secretary or Joint Secretary (in case of emergency during the absence of the home secretary). The "Review Committee" (single committee for both phone tapping and computer data interception) formed under Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 is the same as the one constituted under Rule 419A of Indian Telegraph Act which has a limited number of members. But, there is less clarity in the draft bill regarding who would be the competent authority for interception approval, whether there will be a review committee etc.

However, if the draft bill moves in the same direction as the existing framework, concerns about competency and capacity will linger. Moreover, the authorisation mechanism of interception within the executive wing without parliamentary or judiciary oversight doesn't bring concrete separation of powers.

Recommendations:

1. **Parliamentary Oversight:** The new law must provide for setting up a Multi-Party Parliamentary Standing Committee to oversee the operations of law enforcement agencies and intelligence agencies. A mechanism followed by the UK should advise the model because India inherited and emulated the Westminster model of parliamentary government. The UK has the Intelligence and Security Committee of Parliament[51], formed under the Intelligence Services Act 1994 (reinforced by the Justice and Security Act, 2013[52]) to oversee the policies, expenditure, administration and operations of various intelligence agencies subjected to secrecy.[53] In other democracies such as the UK, the Prime Minister retains control over who will be part of the Committee, provided they are drawn from other parties besides his/her own. In addition, the parliamentarians must be granted access to information related to intelligence and law enforcement agencies operations and procurements without restricting any information under the ambit of

[50] Shekar, K., & Mehta, S. (2022, February 17). *The state of surveillance in India: National security at the cost of privacy?* ORF. Retrieved August 31, 2022, from https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/
[51] *Intelligence and Security Committee of Parliament (ISC)*. (n.d.). Retrieved March 12, 2022, from https://isc.independent.gov.uk/
[52] Justice and Security Act 2013 s. 2 & 3 & sch. I (Ind.).
[53] Official Secrets Act 1989 s. 1(1)(b) (Ind.).

preserving national security, provided there is no conflict of interest, and they maintain secrecy. A similar mechanism is followed by the United States, where the US Congress monitors law enforcement agencies and intelligence agencies, and there are no statutory restrictions on information access.[54]

2. **Judicial Oversight:** The new law should have provisions for judicial authorisation for two reasons (a) prevention and investigation of criminal offences (warrant of interception from the concerned court, with expiry time duration and archiving of intercepted contents and submission to the court). The court warrant must assess the constitutional validity of the request for surveillance through four prerequisites, i.e., legality, legitimate goal, proportionality, procedural guarantees, and (b) a special authority (to be created) for intelligence purposes that can be on the lines of the UK Investigative Powers Commissioner.[55] This authorisation mechanism would bring about a separation of powers to check and oversee. The new legislation should ensure that State agencies (both intelligence and law enforcement agencies) must take a prior warrant from the court to intrude into the private communications between individuals. Various jurisdictions follow this mechanism[56], and India must pick inferences from those to devise a more nuanced judicial authorisation system. The court warrant must access the constitutional validity of the request for surveillance through four prerequisites (as follows) for infringing upon an individual's privacy and personal liberty discussed in Puttaswamy Judgement I.[57] Besides, this judiciary oversight mechanism has to follow the "tatkal" format to expedite the clearance of the interception orders.

3. **Review Committee:** In addition to the external oversight proposed above, the existing review committee model formed under Rule 419A of the Indian Telegraph Act must be revamped in the new legislation, which has the representation of external members and experts. The constituted authority should be answerable to the Parliamentary Committee and the Parliament in general. Also, it should be empowered to take complaints about unauthorised disclosure of classified or sensitive national security information, illegal surveillance activity, administrative misconduct etc.

---

[54] Smist, F. J., Jr. (1994). *Congress Oversees Us Intelligence 2/E: Community 1947-1993* (Second Edition, 2). Univ Tennessee Press.
[55] *IPCO – Investigatory Powers Commissioner's Office*. (n.d.). Retrieved November 8, 2022, from https://www.ipco.org.uk/
[56] Under the Canadian Security Intelligence Service Act, 1985, specially designated judges of the Federal Court provide the approval to the warrant of the intelligence agencies. In the United States, intelligence and law enforcement agencies must take warrants, court orders etc., for domestic surveillance activities under the Electronic Communication Privacy Act of 1986. In addition, in Riley v. California, the United States Supreme Court marked that search and seizure of digital data are considered to be unconstitutional.
[57] *Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors.* [S.K. Kaul, Part J] *(2017)*. Retrieved November 8, 2022, from https://indiankanoon.org/doc/127517806/

These oversight mechanisms would therefore create a separation of powers to check and oversee executive actions, which could sometimes hamper democratic safeguards due to malicious motives.[58]

5.3. Protecting the data

While the procedures limit the duration of the interception, record keeping and usage of intercepted information, it does not limit the amount of data that can be accessed through surveillance. Due to no limitations, the agencies can retrieve data for a lifetime, i.e., from the day an individual uses a phone or internet service without any purpose.

Moreover, over time, surveillance technologies, data processing and analytics tools have evolved massively, which has paved the way for interceptions (intentionally and unintentionally). These developments are concerning in the backdrop of a lack of a data protection regulation in India to protect the informational privacy of individuals. Additionally, the draft Indian Telecommunication Bill does not clarify how personal data and sensitive personal data of individuals and their networks collected through surveillance are protected while processing for investigations.

Besides, law enforcement and investigation agencies store the data received for investigation if the case gets extended and complies with the data retention timeline mandates. However, there is less clarity regarding data storage security and re-use by investigation and law enforcement agencies.

Recommendations:

1. **Technical Safeguards:** Various technical safeguards must be established to protect the privacy of individuals following some of the below universal principles:
    - **Data minimisation:** Minimal data must be collected for the prescribed purpose.
    - **Proportionality:** The data required through surveillance must have a rationale connection with the object of the investigation, such that the data demanded is absolutely necessary. The UK also propagates this principle through its Investigatory Power Act, 2016 (previously Regulation of Investigatory Powers Act, 2000), which mandates that data demanded by intelligence agencies must be necessary and proportionate.
    - **Purpose limitation:** The information received through surveillance must be processed only for the case/investigation it was accrued. The investigating agency must initiate a new request to use the same evidence in other cases/investigations.

[58] Ryan, J. (2009, April 14). *Torture Memo Gave White House Broad Powers*. ABC News. Retrieved March 12, 2022, from https://abcnews.go.com/TheLaw/DOJ/story?id=4569746&page=1

Besides, the usage of evidence for anything other than law enforcement must be prohibited.

- **Privacy by design[59]:** The evidence processing by law enforcement agencies and intelligence agencies should be privacy-friendly and do not trade off privacy at the cost of other State interests such as national security, public order etc. It should use Privacy by Design to ensure that unnecessary personal details are not exposed. The access control must be designed to be adequately granular, with audit trails, to enforce privacy and accountability.
- **Data provenance:** Law enforcement agencies and intelligence agencies must have legal and technical measures to differentiate citizens from foreign nationals within the bulk of data gathered through surveillance. By identifying the provenance of the data, it should be treated differently as Indian citizens have constitutional rights and protections that must be factored in a while using their data
- **Data security:** The data collected through surveillance should be encrypted at rest to ensure the safety of the information stored.
- **Data deletion:** The data collected through surveillance must not be retained longer than necessary, which is followed by intelligence agencies in the UK under Investigatory Powers Act, 2016.[60] The information gathered through surveillance by law enforcement and intelligence agencies must be destroyed at the lapse of data retention mandated by regulations.
- **Data disclosure:** When a crime or security threat is not established from the data collection and processing exercise, the agencies must inform the individuals about the surveillance and reveal the data collected (after a period of time) to them.
- **Fair and lawful processing:** The data acquired through surveillance must be processed fairly and lawfully such that unintended consequences like discrimination, historic disposition, and oppression do not translate into the action.
- **Training**: The personnel engaged in surveillance, including supervisory officials, must attend training on privacy and ethics annually to ensure that the right culture is built and nurtured.

2. **Administrative safeguards:** The new law must ensure that every law enforcement agency and intelligence agency must have privacy/ethics officers within their agencies to ensure day-to-day operations are not violating ethicality and privacy. The officer should also advise and guide the officials on privacy and ethical issues. Many countries,

[59] Internet Architecture Board. *Privacy by design has seven foundational principles*. Retrieved November 8, 2022, from https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
[60] Investigatory Powers Act 2016 s. 87 & 150 (UK).

including the US, UK and Germany, follow this system. For instance, in the US, the Office of Privacy and Civil Liberties is formed within the CIA[61], NSA[62] etc.

5.4. Procuring Interception Technology

Some of the key concerns related to the surveillance from the existing legal framework still linger within the draft bill, such as the lack of provisions that guide the state while procuring tools and software that would secure both privacy and national security. The new bill doesn't have principles guiding the state to determine safe tools for surveillance. For instance, when the state procures an X technology, it is important to ensure that the source code and C&C server of the same is controlled within India.

Recommendations:

1. It is important to ensure that the domain name used by Command and Control (C&C) servers resolves to cloud-based virtual private servers rented by the X technology in India.[63]
2. The Indian government must have visibility of the software's source code and storage policy of the C&C servers while using the technology.
3. The new bill must have principles guiding the state to determine safe tools for surveillance and categorise technology in terms of legal vs illegal.

5.5. Interception of Encrypted Communication

Clause 24 of the Draft Bill replicates the powers under Section 5 of the Telegraph Act, 1885 and gives power to central and state governments to intercept messages and class of messages. This was an opportune moment for the government to come up with comprehensive interception and surveillance laws which put necessary safeguards and checks and balances on the executive power.[64] However, on the contrary, the bill expands the scope of interception to internet-based communications as well. This is not in line with the necessity and proportionality tests laid down in the Puttaswamy judgement. Further, it also needs to be kept in mind that the interception powers under the draft bill will now cover end-to-end encrypted platforms as well.

---

[61] *Office of Privacy and Civil Liberties*. (n.d.). CIA. Retrieved March 12, 2022, from https://www.cia.gov/about/organization/privacy-and-civil-liberties/

[62] *Civil Liberties & Privacy Overview*. (n.d.). National Security Agency. Retrieved March 12, 2022, from https://www.nsa.gov/Culture/Civil-Liberties-and-Privacy/Overview/

[63] Marczak, B., Scott, J., McKune, S., Razzak, B. A., & Deibert, R. (2018, September 18). *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries - The Citizen Lab*. Citizen Lab. Retrieved March 12, 2022, from https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[64] Authorisation and Necessary Safeguards for a surveillance law is discussed in detail in the next section

Impact on End-to-End Encryption

The definition of the "telegraph" has been expanded and defined as "telecommunication services" in the new bill under Clause 2(21), which includes voice mails, video and data transmissions, internet-based communication services etc., creates concerns. The new definition would allow state actors to intercept information transmitted by messaging service providers, voice-over-IP service providers, videotelephony software programs etc. which are traditionally encrypted to secure individuals' privacy. This provision would affect communication businesses that innovate privacy safeguards and privacy-preserving technology and have consumer protection as an integral part of their business model.[65]

Fig 2: Ramifications of Weakening Encryption[66]

Violation of user privacy

It is important to note that the Telecom Regulatory Authority of India had recommended to the Department of Telecommunications in 2020 that the security architecture of end-to-end

[65] Tiwari, P., & Shreya, S. (2020, October 31). *In the Digital Age, Here's How Encryption is Protecting Your Privacy.* The Bastion. Retrieved November 7, 2022, from https://thebastion.co.in/politics-and/in-the-age-of-the-internet-heres-how-encryption-is-protecting-your-privacy/.
[66] Shreya S, Tiwari P. (2020, December), Analysing the American Safe Harbour Regime: Takeaways for India, The Dialogue, Retrieved November 7, 2022 https://thedialogue.co/wp-content/uploads/2020/12/Analysing-the-American-Safe-Harbour-Regime_Takeaways-for-India_The-Dialogue.pdf

encrypted services should not be tinkered with as that would compromise the privacy, safety and security of citizens.[67] Also, indicating a compromise of end-to-end encryption for the state interest, like national security, public order etc., may fail the proportionality and necessity test suggested by the Supreme Court in Puttaswamy Judgement 1.[68] Given that the originator traceability mandate envisaged under Rule 4(2) of the IT Rules, 2021[69] is being contested before the Delhi High Court, it is not ideal for legislating a provision under the Draft Bill with even far-reaching privacy and security implications.

Global Implications

What the interception mandate overlooks is that end-to-end encryption is a system-level design and one that is the same for all users of an application. Forcing communication platforms to enable the interception of messages cannot be a country-specific change for multiple reasons. First, the likes of Signal and WhatsApp have a common application interface and design, and these are not country-specific. Secondly, these platforms enable cross-border communication between users. Such a law in India would put into danger the privacy of all users on these platforms, irrespective of the country.[70] It would also lead to the fragmentation of the internet, with demands for country-specific versions of technologies. Such a scenario would ultimately result in a great deal of disharmony and incompatibility of regulations.

Security Implications

The Dialogue conducted a study on the National Security Implications of Weakening Encryption based on qualitative inputs from experts in law enforcement, intelligence agencies, the military and India's tech community, as well as a deep study of global legal and technical standards.[71] The study identified that the key challenge to catching criminals in cyberspace is not encryption but

---

[67] Telecom Regulatory Authority of India (2018, July 16). *Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector*. Retrieved October 16, 2022, from https://trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

[68] *Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors.* [S.K. Kaul, Part J] *(2017)*. Retrieved November 8, 2022, from https://indiankanoon.org/doc/127517806/

[69] Rizvi, K., & Singh, S. (2021, March 15). *Does The Traceability Requirement Meet The Puttaswamy Test?*. Live Law. Retrieved October 29,2022, from https://www.livelaw.in/columns/the-puttaswamy-test-right-to-privacy-article-21-171181.

[70] United Nations General Assembly (1966 December 16) *Article 17 of the International Covenant on Civil and Political Rights.* Retrieved November 7, 2022, from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights#:~:text=before%20the%20law.-,Article%2017,against%20such%20interference%20or%20attacks. And, United Nations General Assembly (1948 December 10) *Article 12 of the Universal Declaration of Human Rights*. Retrieved November 7, 2022, from https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks

[71] Azad, Y., Venkat Narayanan, A., Tiwari, P., & Chatterjee, S. (2022, January 12). *Analysing the National Security Implications of Weakening Encryption*. The Dialogue. Retrieved November 7, 2022, from https://thedialogue.co/wp-content/uploads/2022/01/Report-_-National-Security-Encryption-_-The-Dialogue-DeepStrat-_-Jan-12-2022.pdf

the inability to utilise even metadata owing to concerns like access to technology and lack of workforce skilled at analysing metadata.

The success of Project Trojan Shield, wherein over 500 criminals were arrested, explains how ingenious use of encryption tech can be utilised to catch criminals. Herein the police planted a compromised encrypted App, 'An0m', in a criminal network to surveil only the bad actors. The project relied on traditional surveillance manoeuvres to target defined actors instead of surveilling everyone.[72]

As savvy criminals shift to unlicensed encrypted Apps to evade detection, ultimately, the interception mandate risks the privacy and security of all users only to catch the not-so-smart criminals. More importantly, the regulated end-to-end encrypted platforms share metadata with law enforcement agencies which helps the latter catch bad actors.[73] If the bad actors get a whiff that messages can be intercepted on licensed platforms, then they will simply shift to an unlicensed secure communication App, and law enforcement would even lose the metadata that they initially received from platforms to aid their investigation. Weakening encryption may also lead to foreign surveillance, espionage and cyber attacks by non-state actors on the sensitive personal data of Indian users.

Business Model

Moreover, intercepting the encrypted communication distorts the core business model of messaging service providers, voice-over-IP service providers, video telephony software programs etc., i.e., to enable secure and encrypted connection over unsecured internet infrastructure. Also, the trust quotient, an integral part of these businesses, will be compromised. Also, the draft Indian Telecommunication Bill does not clarify how this provision would apply to businesses that traditionally do not hold any records of communication. This would make such businesses eventually move towards instrumenting systems and mechanisms that record data, defeating the end-to-end encryption services and causing privacy and security implications.[74]

---

[72]EUROPOL (2021 June 8) *800 criminals arrested in biggest ever law enforcement operation against encrypted communication.* Retrieved November 7, 2022, from https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

[73]Science and Technology Branch, Operational Technology Division (2021 January 7) *Lawful Access: FBI's ability to legally access secure messaging app content and metadata,* Federal Bureau of Investigation. Retrieved November 7, 2022, from https://s3.documentcloud.org/documents/21120480/fbi-doc.pdf

[74] Husain, Y. (2022, October 16). *Big Brother will be watching you: Experts weigh in on privacy dangers of the draft Telecom Bill 2022*. Mid-Day. Retrieved October 16, 2022, from https://origin.mid-day.com/sunday-mid-day/article/big-brother-will-be-watching-you-experts-weigh-in-on-privacy-dangers-of-the-draft-telecom-bill-2022-23250637

Economic Implications

Per a study that analyses the economic implications of weakening encryption technology in Australia[75], it was found that the encryption-hostile law can inflict significant economic harm and produce negative spillovers that amplify that harm globally. In addition to increasing business uncertainty, it also fractures public trust in the Internet and its enabled services.

Recommendations:

- The definition of "telecommunication services" should be considered to ensure that some of the legacy encrypted services like messaging service providers, voice-over-IP service providers, video telephony software programs etc., are exempted from the interception mandates.
- The Department of Telecommunication should consider the economic and geopolitical implications of the interception mandate for businesses that traditionally do not have any communication records.
- The law must clarify how interception provisions would be operationalised by businesses that traditionally do not hold any communication records.

6. Spectrum Management

The government has taken progressive steps in managing spectrum in the country in the draft bill. In line with its stated intent, including special provisions such as deferral and exemptions for entities under distress or insolvency or otherwise unable to pay licence fees for extraordinary reasons is a welcome step as they take into account the representations of the industry to provide relief. This will prompt telecom companies to invest in infrastructure and network expansion, thereby improving customer experience.

Further, the ability to trade, sell or lease spectrum will foster healthy market dynamics and potentially lead to new players entering the sector. Similarly, the move to allow the acquisition of a licensed entity from a non-licensed entity through a notification rather than approval is a welcome move to cut down on deal uncertainty and delays, and the associated terms and conditions will need to align with this concept to avoid diluting the intent. Furthermore, the introduction of re-farming/repurposing, enabling trade and surrender of the spectrum, and the provision to return it to the central government are steps in the right direction.

[75] Internet Society (2021 June 1) *The Economic Impact of Laws that Weaken Encryption*. Retrieved November 7, 2022, from https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/

However, the increased emphasis on the administrative allocation of the spectrum can be revisited to incorporate procedural safeguards and reduce the central government's role in the process in the interest of maintaining player parity in the industry. Such a step will reinforce players' confidence in the industry and ensure more equitable competition benefitting all stakeholders. The central government has been accorded additional powers to themselves through the draft bill to play the role of the regulator, operator (through MTNL and BSNL) and also the licensor. Such an expanded role can adversely affect player parity in the industry and disincentivise new players from entering the market. As a result, it is recommended that this expanded role be revised in accordance with principles of player parity to ensure that all stakeholders stand on a level playing field.

Additionally, about 30% of the revenue of telecom operators is paid towards spectrum charges, including annual fees. The spectrum pricing formula also needs to be revised in order to relax the pressure on telecom operators. With an expansive customer base in this decade, services provided to customers in current times are varied and require more data - and therefore, telecom operators require access to larger amounts of spectrum. The existing mechanism is based on per megahertz, which does not allow telecom operators to address the increased demands of customers. Other areas of focus include infrastructure creation (which includes the laying of optic fibre) and quality of services. Tier II and Tier III cities still suffer from poor connectivity and unreliable internet connectivity.[76] The Universal Service Obligation Fund (USOF) or its proposed new title, 'Telecommunication Development Fund (TDF)', can be focused on enabling government and industry stakeholders to work collectively towards this goal.

Recommendations:

1. Include procedural safeguards in the administrative allocation of spectrum
2. Re-visit the expanded role of the central government in the interest of player parity in the telecommunications services industry.
3. Mandate auction of the spectrum as the primary mode of spectrum allocation due to its price discovery role.

7. Telecommunication Development Fund

The draft bill proposes renaming the Universal Service Obligation Fund (USOF) as the 'Telecommunication Development Fund (TDF)', which will be undertaking the same responsibilities as its predecessor with the scope expanded to include economically unviable areas in urban areas, promoting equipment manufacturing, funding pilot projects for driving

[76]Tripathi, A., Vaidyanathan, M., Pande, T., (2021) *Enabling a Trillion Dollar Digital Economy: Interdependent, Interconnected and Digital*. The Dialogue and ASSOCHAM. Retrieved on October 18, 2022, from https://thedialogue.co/wp-content/uploads/2021/02/Enabling-a-Trillion-Dollar-Economy-The-Dialogue.pdf

innovation. The proposed Telecommunication Development Fund must first address its predecessor's unutilised fund issue. Around $6.7 Billion (₹50,000 Crore) of the USOF is currently unutilised[77], while a major improvement in access to telephony and the internet across India is driven primarily by private investment.

At present, 25,067 inhabited villages still do not have mobile network coverage, and this presents a significant obstacle in India's push toward a digital future.[78] While BharatNet and other initiatives funded by USOF have shown great progress in increasing coverage, they often provide unreliable and slow connections to these regions such that it does not benefit them in the long run as most sites are nonfunctional in 2G mobile network speeds. Allowing private companies to build and maintain infrastructure in collaboration with the government would significantly increase our network coverage timelines and help reduce costs.

Collaboration of public and private entities through the newly proposed Telecom Technology Development Fund (TTDF)[79] Increasing access to services and elevating consumer experience is a step in the right direction towards enabling collaboration between private and public stakeholders.

Additionally, besides the high spectrum auction costs, the government levies in the telecom sector, estimated to be 30% of their revenues, are among the highest in the world.[80] The Department of Telecommunications (DoT) levies three kinds of fees and charges: (i) initial entry fee, which is non-refundable, (ii) annual licence fee, which includes a contribution to universal service obligation (now TDF); and (iii) spectrum usage charges. Idle funds under the TDF can be mobilised to address this issue.

Recommendations:

1. Channel idle funds for collaborative projects with industry and government stakeholders in order to increase quality access to telecommunications services across the country.
2. Enable collaboration between stakeholders to maintain and revamp telecommunications infrastructure across the country.
3. Include private players in the deployment process to achieve the fund's objectives of enabling innovation, funding new technologies and increasing network coverage area.

---

[77] Department of Telecommunications (2022 August 31) *Fund Status of the Universal Servicee Obligation Fund*, Ministry of Communications. Retrieved November 15, 2022, from https://usof.gov.in/fund-status
[78] Minister of State for Communications (2021 August, 4) Lok Sabha Unstarred Question No. 2672, Lok Sabha. Retrieved on August 30, 2022, from http://164.100.24.220/loksabhaquestions/annex/176/AU2672.pdf
[79] Universal Service Obligation Fund (2022 October 1) *Universal Service Obligation Fund (USOF) launches Telecom Technology Development Fund scheme*. Department of Telecommunications. Retrieved on October 29, 2022, from https://pib.gov.in/PressReleasePage.aspx?PRID=1864133#:~:text=Universal%20Service%20Obligation%20Fund%20(USOF)%2C%20a%20body%20under%20the,aligned%20with%20Prime%20Minister%2C%20Shri.
[80] *Ibid.*

8. Amendment to the TRAI Act

Clause 46 of the draft telecom bill brings certain amendments to the Telecom Regulatory Authority of India Act 1997. Clause 46(f) seeks to delete the *proviso* to Section 11(1) of the TRAI Act, which mandates that the central government will seek the inputs of TRAI with respect to the issuance of new licences. Clause 46(g) seeks to delete the proviso to Section 11(1) of the TRAI Act, which mandates that TRAI can request such documents as necessary to make its recommendations. Essentially, clauses 46(f) to 46(i) seek to remove the consultation process between the central government and TRAI regarding the issuance of new licences. Further, clause 46(d) seeks to remove the *proviso* to section 4 of the TRAI Act, which sets the eligibility criteria for appointment as a chairman of the authority. Currently, the provision requires that no one below the rank of secretary and additional secretary to the central government of India can be appointed.

All these amendments to the TRAI Act seek to dilute the power of TRAI in matters of importance. The rationale behind removing certain provisions from the TRAI act, as given by the Minister of IT, was to simplify the processes and minimise the back-and-forth between the two governing bodies.[81] While the intention behind coming up with this provision is good, it is also important that these two bodies work together to enable growth and innovation in the market. The to-and-fro between the two governing bodies is important to ensure checks and balances. Further, as an independent regulator, TRAI plays a critical role in ensuring fairness and accountability, therefore any change in its constitution must be done only after consultation with the authority itself.[82]

Dilution of powers of sectoral regulators and giving overarching powers to one organ of the State undermines the principles of checks and balances and separation of power. While national security is undeniably a legitimate concern, ensuring appropriate checks and balances on the powers of the state is critical to preserve the fundamental rights of the citizenry and upholding the principle of constitutionalism. It is important that there is a constant dialogue between the two governing bodies, and at the same time, the autonomy and independence of TRAI is maintained.

[81]Guha, K., Rathee, K. (2022, October 31). *Trai needs more teeth to punish and enforce: Ashwini Vaishnaw*. The Economic Times. Retrieved November 8, 2022, from https://economictimes.indiatimes.com/industry/telecom/telecom-news/trai-needs-more-teeth-to-punish-and-enforce-ashwini-vaishnaw/articleshow/95187460.cms

[82]Goled, S. (2022, November 7). *Will Proposed Amendments to TRAI Act Reduce the Body to Toothless Tiger?* Analytics India Magazine. Retrieved November 8, 2022, from https://analyticsindiamag.com/will-proposed-amendments-to-trai-act-reduce-the-body-to-toothless-tiger/

Recommendations:

1. The provisions, specifically clause 46(d), 46(f), 46(g), 46(h), and 46(i), should be deleted from the draft bill as it seeks to dilute the power of TRAI. A constant dialogue between the two authorities is important to ensure checks and balances.

9. Offences

Clause 47, read with schedule 3 of the draft bill, provides for punishment and penalties in case of a contravention. Schedule 3 enumerates that an entity providing telecommunication services or telecommunication network operating without obtaining licences will have to face imprisonment for up to 1 year or 50 Lakhs or both. Further use of unlicensed telecommunication services by any entity would also attract penalties. Alarmingly, schedule 3 also provides that a person or a user can be penalised up to 1 Lakh for the continued usage of unlicensed telecommunication services on the ground of 'having reason to believe so".

Imposing criminal liability on entities in a civil matter is excessive; instead, punitive action could be appropriate and proportionate to hold the entities accountable for any offence. Further, there is no rationale for penalising users for continued usage of unlicensed services. This would open a pandora's box of litigation and unnecessary imposition of penalty. Further, the ground for penalising the user itself is ambiguous and may be misused as the burden will be on the user to prove a lack of knowledge of whether the app is licensed or not.

Clause 51 further provides power to search and seizure of licensees of a telecommunication service to disclose any information that is in its possession or control sought by the government through its authorised officers. The wide clause empowers the government to mandatorily seek any information pertaining to telecommunication services, networks and infrastructure.

Provisions for search and seizure exist under section 91 of the Code of Criminal Procedure 1973 (CrPC) and clause 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Under these statutes, authorised officials can seek certain information that may aid and assist the enforcement agency in any pending or apprehended civil or criminal proceedings. However, in both cases, the language of the provisions provides greater specificity that restricts the number of people that have access and places responsibilities on such officers to protect such data or information received. Contrary, the draft Bill provides additional avenues for law enforcement authorities to conduct search and seizure – this could lead to arbitrary use or misuse of power by the government.

Recommendations:

1. Remove penal actions on the users of the telecom services.
2. Remove criminal liability on the entities as it will impact innovation and the ecosystem's growth.
3. The power of search and seizure already exists under other laws. Therefore there is no rationale behind putting another provision in this bill.

10. About The Dialogue

The Dialogue™ is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry on issues concerning technology policy. The Dialogue™ has been ranked as one the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania, in their 2020 and 2021 rankings.

Visit our website here - www.thedialogue.co

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

https://thedialogue.co