



The Dialogue™
INFORM ENGAGE IDEATE

To,
Mr. Akhilesh Kumar Trivedi,
Advisor (Networks, Spectrum and Licensing), Telecom Regulatory Authority of India,
New Delhi, India

Dear Sir,

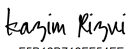
On behalf of The Dialogue, I am writing to express our sincere gratitude to the Telecom Regulatory Authority of India (TRAI) for the opportunity to submit comments on the consultation paper on 'Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services' dated July 7, 2023.

Notably, we would like to highlight the following major aspects in our submission:

- Classification of OTT communication services are not required at the current stage. The dynamic nature of OTT services leads to an inherent overlap of functions, rendering straight-jacketed classification approaches futile.
- Internet services and Telecommunication services cannot be equated together given that they are distinguishable on structural, functional and technical levels. Accordingly, OTT communication services and Telecom services should not be regulated together.
- A licensing regime, while organised, could stifle innovation by imposing high compliance costs, thereby impeding the growth of start-ups. Given the rapid evolution of OTT services, a static regulatory regime could severely hamper progress in this dynamic field.
- Imposing a network usage fee would severely impact the operational costs of OTT services and pose a potential threat to net neutrality principles. Additionally, consumers would also bear the brunt of this fee as it would be passed on to them.
- OTT services have become integral in today's digital world, supporting activities like remote work, education, and business. Suggesting a selective ban on these platforms can cause considerable disruption and raise various technical, legal, and ethical concerns.

We have mentioned our detailed response on all these aspects and we sincerely hope that our recommendations will contribute to the development of a forward-thinking regulatory framework for India's technology space.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact us anytime. We would also be happy to offer our inputs and insights directly through meetings and discussions with the relevant authorities as well.

DocuSigned by:

F5B12B712FF54FE...

Kind regards
Kazim Rizvi
Founding Director



The DialogueTM
INFORM ENGAGE IDEATE

Comments on TRAI Consultation Paper
On
Regulatory Mechanism for Over-The-Top (OTT) Communication
Services, and Selective Banning of OTT Services

Authors: Ayush Tripathi, Shruti Shreya, Bhavya Birla

I. Introduction

Digital economy is a key enabler to India's vision of becoming a trillion dollar economy. A free and open internet which gives opportunity to the new entrants in the market and gives scope for innovation is going to be very important in this Techade as envisioned by Hon'ble Prime Minister. Therefore, it is important to enable innovation and growth of the internet through supportive policymaking to achieve the larger goal of Digital India.

The consultation paper by TRAI titled "Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services" ('Consultation Paper') explores the need for regulations for OTT communication services and also delves into the mechanism for putting ban on selected OTT services which are found to be in contravention with the existing laws. This paper is the latest initiative in the series of consultation papers brought by TRAI to regulate OTT communication services at par with the telecom service operators. In furtherance of these efforts, The Dialogue published a comprehensive report titled "Convergence of Internet and Telecom Services: Assessing the Impact on Digital Ecosystem".¹ The report delved into the issues relating to convergence and argued for status quo on the regulation of OTT services. It also discussed the impact of network usage fee on OTT services and consumers alike. The report answers the majority of the questions posed by this consultation paper.

The consultation paper argues for regulation of OTT communication services at par with the telecom which may pose problems in the Indian context. The paper essentially seeks to bring licensing of internet services at par with telecom and broadcasting services and under a single regulator. It is important to note that TRAI's power is limited to carriage in telecommunication services while according to Allocation of Business Rules, powers related to broadcasting services rests with the Ministry of Information and Broadcasting which has been regulating the subject matter. Further, regulation of internet services comes within the ambit of the Ministry for Electronics and Information Technology and OTT Communication apps are regulated through Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

We believe that there are apt laws to regulate the OTT Communication services and licensing regime for the internet will only lead to increased entry barriers, deter innovation, negatively impact ease of doing business and ultimately impact consumers who may have to pay for the increased charges. We believe that instead of a converged regulation, there is a need for greater coordination and harmonisation among the regulators i.e TRAI, DoT and MeitY to work towards a safe, secure and accountable internet. If there is a need for a set of regulations, it should come after inter-ministerial discussions and from ministries responsible for such domain. Towards this, following are the answers to the questions posed for consultation.

¹ Tripathi A, Rizvi, K, Sahiba, J, Birla B (2023), Convergence of Internet and Telecom Services: Assessing the Impact on Digital Ecosystem, The Dialogue, Retrieved from: https://thediologue.co/wp-content/uploads/2023/06/RESEARCH-REPORT_-Convergence-of-Internet-and-Telecom--The-Dialogue.pdf

II. EXAMINATION OF THE ISSUES RELATED TO REGULATORY MECHANISM FOR OTT COMMUNICATION SERVICES

Answers to Q.1 - Q.5: Classification and Regulation of OTT Communication Services

At the outset, we would like to submit that classification of OTT communication services are not required at the current stage. In the current digital landscape, the nature of OTT services has evolved to encompass multifaceted functions within a single platform. Unlike traditional frameworks where services could be easily categorised into distinct compartments, the modern reality paints a different picture. Today, an individual OTT platform might undertake an array of functions that transcend the confines of traditional categorisation.

Attempting to fit these versatile and dynamic platforms into predetermined, rigid categories becomes increasingly obsolete. The dynamic nature of OTT services leads to an inherent overlap of functions, rendering conventional classification approaches futile. In this context, the notion of adhering to a straight-jacketed formula for categorisation will be counterproductive, failing to capture the intricate interplay of roles these platforms assume.

While a principle-based regulatory approach is paramount for governing OTT platforms, the endeavour to classify them into distinct categories should be avoided. Moreover, under the IT Act, OTT services are already subjected to a catena of regulations which are sufficient to govern all their functional aspects. Any further regulation envisaging a classification approach will inevitably falter in capturing the nuances of these platforms' operations and their transformative nature in the digital age.

By avoiding attempts at strict classification, regulators can better focus on fostering an environment that promotes innovation, consumer protection, and fair practices, allowing the diverse functions of OTT platforms to flourish without unwarranted constraints.

Further, we believe that Internet services and Telecommunication services are inherently different from each other on fundamental levels. These two services cannot be equated together given that they are distinguishable on structural, functional and technical level. OTT communication services are already regulated under the Information Technology Act, 2000 and allied rules. Further, the upcoming Digital India Act will also regulate the OTT communication services at large. Therefore, for the reasons given below, we submit that OTT communication services and Telecom services should not be regulated together.

A. Spectrum is a natural resource, while the Internet is not

Telecom and Internet services are fundamentally distinct. The rationale behind regulating Telecommunication Service Providers ('TSPs') through licensing requirements is based on economic grounds and 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)*², *Union of India v. Centre for Public Interest Litigation (2012)*³, and *Bharti Airtel v Union of India (2015)*⁴ 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 spectrum usage and intervene when necessary.

Article 39(b) of the Indian Constitution provides that the State needs to direct its policy towards ensuring that 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 resources, but are services which are provided utilising the services that distribute spectrum. While spectrum is a natural resource, internet services which work on the application layer are not because (a) there is no scarcity as it is, to an extent, non-rivalrous, and (b) there is a market where private players are already competing at the application layers.

B. ‘Same Service, Same Rules’ Argument is not Applicable

Often, the argument of “same service, same rules” has been raised⁵, 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. This argument lacks merit 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 vs. 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.

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

² *Ministry of Information and Broadcasting v Cricket Association of Bengal and Ors*, AIR 1995 SC 1236.

³ *Centre for Public Interest Litigation and Ors. v Union of India*, (2012) 3 SCC 1.

⁴ *Bharti Airtel v Union of India (2015) 12 SCC 1*.

⁵ PTI (2022, October 26) *COAI Roots For 'Same Service, Same Rules' For Parity With OTT Communication Services*, Outlook India. Retrieved on May 20, 2023 from <https://www.outlookindia.com/business/coai-roots-for-same-service-same-rules-for-parity-with-ott-communication-services-news-232550>

OTT services to provide their services in the absence of TSPs. As enumerated below, the two services have inherent structural, technical and functional differences.

C. Structural and Technical Differences between Telecom and OTT Services

OTT service providers and TSPs function on fundamentally different technical foundations. 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 Public Switched Telephone Network ('PSTN') architectures, where dedicated communication channels are established between devices for the duration of the communication.⁶ 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 services and network access. There are numerous examples available in the public domain where TSPs have ventured into the online streaming platforms. 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.⁷ 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 Media Access Control ('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

⁶ Ikigai Law (2019, August 6) 'Over-The-Top' And 'Telecom' Services – Similar Or Not? - Our Analysis Of Stakeholders' Responses To Trai Consultation Paper. Retrieved on 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>

⁷ O'Keefe, A. (2022, May 16) *OSI layers: Everything you need to know*, Aussie Broadband. Retrieved on October 13, 2022, from <https://www.aussiebroadband.com.au/blog/osi-layers-everything-you-need-to-know/>

area network ('VLAN') communications. This dual-layer functionality is why a Layer 3 switch is also known as a multilayer switch.⁸

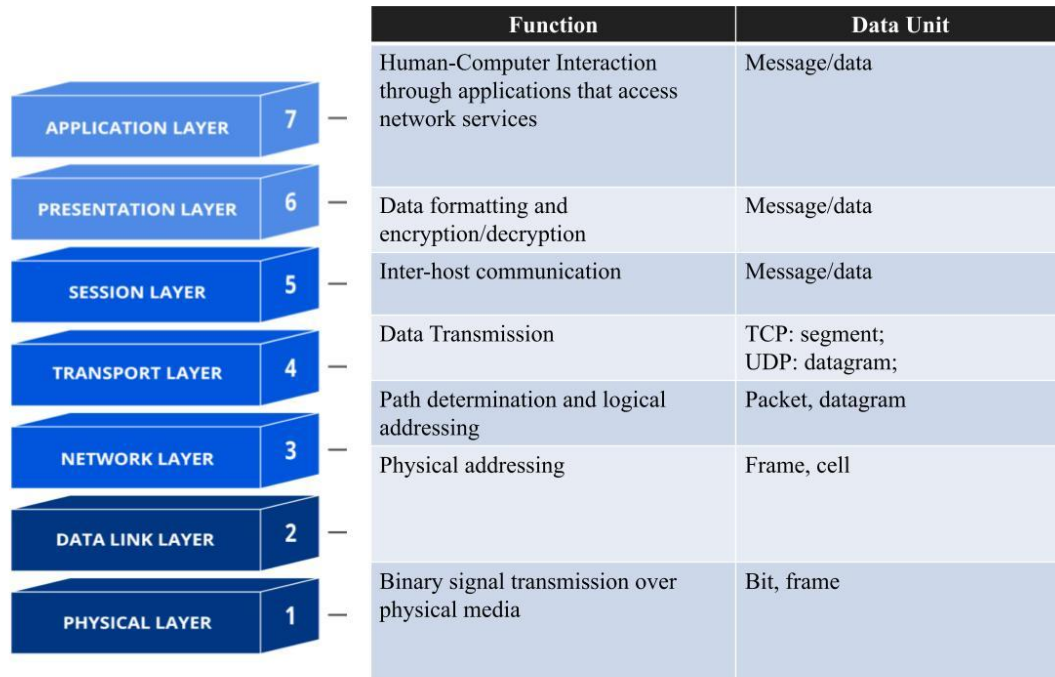


Fig. 2: Open System Interconnection Model

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 a 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.⁹

⁸ O'Keeffe, A. (2018, October 20) *The difference between Layer 3 and Layer 2 networks*, Aussie Broadband. Retrieved on October 13, 2022, from [https://www.aussiebroadband.com.au/blog/difference-layer-3-layer-2-networks/#:~:text=A%20Layer%20%20switch%20only,area%20network%20\(VLAN\)%20communications.](https://www.aussiebroadband.com.au/blog/difference-layer-3-layer-2-networks/#:~:text=A%20Layer%20%20switch%20only,area%20network%20(VLAN)%20communications.)

⁹ Asia Internet Coalition (2018, December 28) *Submission on the Consultation Paper on Regulatory Framework for Over-The-Top (OTT) Communication Services in India*. Retrieved on October 13, 2022, from <https://traf.gov.in/sites/default/files/AsiaInternetCoalition08012019.pdf>.

The TRAI 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. 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.¹⁰

These technical differences demonstrate 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.

D. Functional Differences

Services offered by OTTs and TSPs are distinct in nature. While there is overlap in the communication services on aspects such as 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.

To suggest that there is a natural parity or similarity between OTT players and 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 any additional licence. In contrast, 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.¹¹ OTT provides rich interactions beyond text and voice communication on the application layer, and that's the innovation which should not be curbed.

¹⁰ TRAI (2017, October 24) *Recommendations On Regulatory Framework for Internet Telephony*. Retrieved on October 15, 2022, from https://traigov.in/sites/default/files/Recommendations_24_10_2017_0.pdf

¹¹ Broadband India Foundation (2017, April 27) *Counter Comments from BIF on TRAI consultation paper on Net Neutrality*. Retrieved on October 13, 2022, from https://traigov.in/sites/default/files/BIF_27_04_17.pdf

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. As a result, asking for regulatory parity on the basis of the “same service, same rules” argument is incorrect and does not justify a higher regulatory burden on OTT players.

Q6. Regulation of OTT Communication Services

Answer:

The creation of a licensing regime for providers of OTT communication services has been a consistent demand of traditional telecom service providers. 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. There is also no clarity on whether there will be a distinct licensing regime for TSPs and OTT communication services in the Draft Bill. Because if they are considered the same, then OTTs will also be able to acquire spectrum, and if there are distinct agreements, then these two services cannot be considered substitutable.

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”. It will undoubtedly increase entry barriers for new players and impact the growth curve of an emerging sector. It 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. Internet-based services also have to comply with the IT Act, 2000 and other sectoral laws. 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.

A. Overlaps of Jurisdiction

Apart from the fundamentally distinct nature of these two services, another important reason for recommending the exclusion of internet-based services from the ambit is that they are already regulated by the Information Technology Act, 2000 (IT Act, 2000). 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/regulators 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 an overwhelming financial burden. This could hamper innovation and consumer choice.

OTT service providers are already subject to existing laws governing interception, privacy, cybersecurity, etc., under 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 2022¹², 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 Ministry of Information and Broadcasting ('MIB').

Overlaps with Existing laws

S.No.	Existing and Proposed Legislations	Existing Provisions	Overlaps with Telecom Bill
1.	Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009	Rule 3 enables a government official to order the interception, monitoring or decryption of any information generated or transmitted over a computer resource	Clause 24(2)(a) of the Draft telecom bill empowers authorised government officials to intercept, detain or seek disclosure of a message or a class of messages in the interest of public order and national sovereignty. Due to the broad definition of 'telecommunication services' this applies to all common messaging platforms and a host of other online communication services.
2.	Information Technology (the Indian Computer Emergency Response	Rule 11 establishes the gradational approach to CERT-IN's resource allocation in cases of	Clause 25 enables the Central government to take control of telecommunication infrastructure, or telecommunications services

¹² 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.

	Team and Manner of Performing Functions and Duties) Rules, 2013	cyber security incidents.	and prescribe standards, or procure necessary infrastructure or even allocate all these powers to another government authority in cases of war or in the interest of national security.
3.	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021	Rule 4(2) mandates Significant Social Media Intermediaries ('SSMIs') to enable the identification of the 'first originator' of a message within the Indian territory.	Clause 24(2)(a) empowers the central government to seek disclosure of a class of messages or a message in the interest of national security. While the clause does not mention 'originator' of the message, in essence it allows the central government to seek disclosure of the contents and parties involved in the message chain.

In 2020, 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.

Q7. Licensing/Regulatory Framework for OTT Communication Service vis-a-vis Telecommunication Services

Answer:

At the outset, we would like to submit that there are apt laws under the current regime to govern every aspect of OTT communication Services. As expounded in Q6, Information Technology Act, 2000 and Information Technology (Intermediary Guidelines and Social Media Ethics Code) Rules, 2021 extensively regulates the OTT communication services including aspects of grievance redressal. Along with this, the recently enacted Digital Personal Data Protection Act, 2023 covers the regulation of protection of data as well.

(a) Lawful interception and (b) Privacy and Security

Bringing OTT communication services at par with the obligations of telecom service providers will defeat the purpose of privacy and security. Consequently, state actors would gain the ability to intercept information transmitted through encrypted messaging services, voice-over-IP providers, video telephony software, and similar platforms. In the absence of any comprehensive laws for surveillance and checks and balances, giving a wider range of services for lawful interception would pose a threat to communication businesses that prioritise privacy safeguards and privacy-preserving technology, with consumer protection as a core aspect of their business model.¹³ *In Arguendo*, the power of lawful interception is already given in Section 69 of Information Technology Act, 2000 and Rule 4(2) of the Information Technology (Intermediary Guidelines and Social Media Ethics Code) Rules, 2021. There is no need for additional obligations in terms of lawful interception for OTT services.

Further, keeping OTT communication services at par with TSPs will have detrimental impact on the End-to-End Encrypted Services for the reasons given below:

Impact on End-to-End Encryption

A. Violation of user privacy

It is important to note that the TRAI had recommended to the DoT in 2020 that the security architecture of end-to-end encrypted services should not be tinkered with as that would compromise the privacy, safety and security of citizens.¹⁴ Also, indicating a compromise of end-to-end encryption for the state interest, like national security, public order etc. may fail the

¹³ Tiwari, P., & Shreya, S. (2020, October 31). In the Digital Age, Here's How Encryption is Protecting Your Privacy. The Bastion. Retrieved on November 7, 2022, from

<https://thebastion.co.in/politics-and/in-the-age-of-the-internet-heres-how-encryption-is-protecting-your-privacy/>

¹⁴ Telecom Regulatory Authority of India (2018, July 16). *Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector*. Retrieved on October 16, 2022, from

https://traai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

proportionality and necessity test suggested by the Supreme Court in Puttaswamy Judgement 1.¹⁵ Given that the originator traceability mandate envisaged under Rule 4(2) of the IT Rules, 2021¹⁶ 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.

B. 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, which are not country-specific. Secondly, these platforms enable cross-border communication between users. Such a law in India would endanger the privacy of all users on these platforms, irrespective of the country.¹⁷ 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 disharmony and incompatibility of regulations.

C. Security Implications

In 2022, the Dialogue conducted a study on the National Security Implications of Weakening Encryption based on qualitative inputs from law enforcement, intelligence agencies, the military and India's tech community experts, as well as a deep study of global legal and technical standards.¹⁸ The study identified that the key challenge to catching criminals in cyberspace is not encryption but 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 the ingenious use of encryption technology can aid in catching criminals. Herein the police planted a compromised encrypted App, 'An0m', in a criminal network to surveil only the bad

¹⁵ *Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors.* [S.K. Kaul, Part J] (2017). Retrieved on November 8, 2022, from <https://indiankanoon.org/doc/127517806/>

¹⁶ Rizvi, K., & Singh, S. (2021, March 15) *Does The Traceability Requirement Meet The Puttaswamy Test?* Live Law Retrieved on October 29, 2022, from <https://www.livelaw.in/columns/the-puttaswamy-test-right-to-privacy-article-21-171181>.

¹⁷ United Nations General Assembly (1966, December 16) *Article 17 of the International Covenant on Civil and Political Rights*. Retrieved on 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 on November 7, 2022, from <https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012.against%20such%20inference%20or%20attacks>

¹⁸ Azad, Y., Venkat Narayanan, A., Tiwari, P., & Chatterjee, S. (2022, January 12). *Analysing the National Security Implications of Weakening Encryption*. The Dialogue. Retrieved on November 7, 2022, from <https://thediologue.co/wp-content/uploads/2022/01/Report--National-Security-Encryption--The-DIALOGUE-DeepStrat--Jan-12-2022.pdf>

actors. The project relied on traditional surveillance manoeuvres to target defined actors instead of surveilling everyone.¹⁹

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 to catch bad actors.²⁰ 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.

D. Business Model

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, gets compromised. Also, the Draft 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 purpose of end-to-end encryption and causing privacy and security implications.²¹

E. Economic Implications

According to a study that analyses the economic implications of weakening encryption technology in Australia²², 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.

¹⁹EUROPOL (2021, June 8) *800 criminals arrested in biggest ever law enforcement operation against encrypted communication*. Retrieved on 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>

²⁰ 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 on November 7, 2022, from <https://s3.documentcloud.org/documents/21120480/fbi-doc.pdf>

²¹ 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 on 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>

²² Internet Society (2021, June 1) *The Economic Impact of Laws that Weaken Encryption*. Retrieved on November 7, 2022, from <https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/>

Q.8. & Q.9: Collaborative Framework for OTT and Telecom Services and Network Usage Fees

Answer:

The digital ecosystem is complex, ever-evolving, and interdependent. While ensuring fairness and open access is crucial, introducing a singular regulatory framework for OTT and TSP collaboration will pose more challenges than solutions. The current market-driven collaborative mechanisms already in place demonstrate that the two sectors can, and do, work together without stringent regulatory intervention. To maintain the dynamism and growth potential of the digital space, it is vital to tread cautiously when considering additional regulatory frameworks.

- **Anti Competitive Concerns:** A formal regulatory framework mandating collaboration might place TSPs in an advantageous position, potentially allowing them to extract anticompetitive benefits from OTTs. By doing so, TSPs could act as gatekeepers to the internet, putting newer or smaller OTT players at a disadvantage and potentially stifling innovation. From a competition lens, a potential risk needs to be discussed. TSPs with sufficient market power may be able to engage in discriminatory pricing and offer preferential terms to select OTTs in the context of network usage fees. Further, this could also impact smaller players who find the network usage fee unaffordable, which could impact fair competition in the market. This situation becomes more concerning given that certain TSPs also have their OTT applications and these applications will be at an advantageous position and will not have to pay any network fees to the parent telcos.
- **Impact on Net Neutrality:** The principle of Net Neutrality has emerged as a central topic in Internet governance forums over the past decade. Various jurisdictions, including India, the United States of America, and the European Union, among others, have engaged in discussions and independently asserted that the Internet should uphold neutrality. However, the collaborative framework may introduce new challenges to preserving net neutrality. Net neutrality is a fundamental principle that ensures the freedom of expression on the Internet, regardless of the Internet Service Provider (ISP) through which one accesses it. It guarantees that the reach and access to online services are not discriminated against by network operators. This principle forms the bedrock of the functioning of the modern Internet. In the absence of net neutrality, platforms are incentivised to compete by forming exclusive partnerships with popular Content and Application Providers (CAPs) in order to gain market dominance. Consumers encounter significant entry barriers as different network operators provide distinct services, each behind their respective paywalls, thereby limiting the consumer's ability to utilise the Internet effectively.

In countries without collaborative framework requirements, Telecommunications Service

Providers (TSPs) operate within a one-sided market where their pricing only impacts their market share and service usage. However, with the introduction of cost-sharing mandates, the network market transforms into a two-sided market, where ISPs negotiate fees not only with users but also with CAPs. This further complicates the already intricate relationships between network providers, CAPs, and end-users, without offering any evident benefits to users. The reason behind this lies in the fact that when network operators demand usage fees from CAPs, these costs are likely to be partially passed on to end-users, as they depend on the uninterrupted flow of services from CAPs. For example, if a usage fee is imposed on a streaming CAP, they may be discouraged from investing in codec optimisation or establishing localised Content Delivery Networks (CDNs) to enhance the end-user experience, ultimately resulting in a detriment to the user. Such practices are already observable in jurisdictions like South Korea, where CAPs have reduced investments in optimising the end-user experience to cover increased compliance costs.²³

In such cases, as has been experienced earlier, organisations enter into exclusive agreements to offer a popular service to their consumers in an attempt to boost market share. Such a scenario may result in throttling of services for non-subscribed users, fragmenting and fundamentally breaking the internet. Thus, any policy interventions mandating a cost-sharing between CAPs, end users and network operators must consider these consequences for the future of the internet too.

- **Impact of Cost-sharing mandate on Consumers: Impact of Cost-Sharing Mandates on Consumers:** Cost-sharing mandates have consequences for all stakeholders involved. Considering consumers are the most important cog in the machine that is the internet, ensuring that consumers are able to access the internet in a fair and transparent manner becomes crucial. Cost-sharing mandates have multiple consequences for consumers:-
 - **Access to services:** Cost-sharing mandates have resulted in a price increase in broadband plans as CAPs in cost-sharing models often push the costs mandated on them onto the consumer. This results in a steep rise in barriers to entry and may negatively impact the internet penetration that has boomed in India owing to the government and industry's collaborative effort to make the internet cheap and accessible nationwide.
 - **Additional Cost:** Cost-sharing mandates have resulted in reduced competition in network operator markets and have, in particular, affected small-medium ISPs that

²³ (2022, November 7) *Consumers Are the Ones Who End Up Paying for Sending-Party-Pays Mandates*. Information Technology and Innovation Foundation. Retrieved from: <https://itif.org/publications/2022/11/07/consumers-are-the-ones-who-end-up-paying-for-sending-party-pays-mandate/>

are not able to keep up with additional costs brought on by network sharing models and are forced by market forces to consolidate with bigger network operators. Because of this consumers are impacted in various forms in a monopolistic market. They lose their ability to negotiate prices as is seen to be present in competitive markets where network operators have to compete with one another over price, resulting in the consumer getting the best price for availing access to the internet. Further, decreased competition has in the past led to discriminatory services from ISPs and has affected consumers unilaterally by increasing costs of entry while decreasing the quality of service.²⁴ As indirect costs increase with Network Cost Sharing, the price of the services and commodities provided by OTT would increase, ultimately hampering the demand curve as India is a price-sensitive market. Therefore, such sensitivity would further corner OTT platforms, especially start-ups, to take on the additional compliance burdens and costs associated with the Network Use Cost as they can't pass it on to their consumers.

- **Decreased quality of service:** Cost-sharing mandates have fallout consequences for the quality of service that ISPs are able to provide their consumers. **In South Korea, for instance, consumers are now forced to pay the same amount for relatively lesser quality services owing to the costs brought on by their SPNP model.** In such models, ISPs are disincentivised from positioning themselves downstream of popular content platforms. They pass those added costs to the content providers as higher traffic volumes are penalised under the SPNP model. The SPNP model has also resulted in ISPs choosing not to host higher quality content (4K movies, shows etc.) as they cost significant traffic. The policy resultantly has impacted the consumers adversely by limiting their choices and decreasing the quality of service.
- **Significant Investments by OTT Providers:** OTT services, particularly the major players, are investing heavily in complementary internet infrastructure. This includes caching through Content Delivery Networks (CDNs) to optimise content delivery, partnering in submarine cable initiatives for better connectivity, and adapting content streams based on network capacity. Such investments are essential to ensure that internet services are efficient, adaptive, and user-centric. Despite the significant increase in internet traffic over the past decade, the voluntary interconnection regime remains a fundamental building block for maintaining a global and interoperable internet based on cooperation between stakeholders operating within a competitive environment. Proponents of network usage fees fail to acknowledge the efforts already being made by

²⁴ Trostle, H., Mitchell, C., Razafindrabe, Ny., Andrews, M., Kienbaum, K.(2020). *Profiles of Monopoly: Big Cable and Telecom*. Institute for Local Self-Reliance. Retrieved from: https://cdn.ilsr.org/wp-content/uploads/2020/08/2020_08_Profiles-of-Monopoly.pdf

CAPs to alleviate the strain on ISP networks and enhance the user experience, both within their own networks and in collaboration with TSPs.

However, if we briefly assess the literature around the investments made by stakeholders in the content layer, this argument begins to lose ground. **As per international studies, stakeholders from the content layer have invested over USD 883 Billion over the last decade. Between 2018 and 2021, content and application providers invested over USD 120 Billion annually and have consistently invested in building and maintaining critical parts of the Internet infrastructure since 2014.**²⁵ This data suggests the increasing contributions made by OTT players in the growth of the global internet ecosystem, thereby facilitating innovation, growth in connectivity, and development of new content and applications.

Further, stakeholders from the content layer have focussed their investments on three main clusters of the internet infrastructure

1. hosting (i.e. data centres and Content Delivery Networks ('CDNs')),
2. transport (i.e. submarine and terrestrial cables), and
3. delivery (i.e. peering and caching).²⁶

This infrastructure for hosting, transporting and delivering content to consumers spans tens of thousands of miles around the globe. It is critical to deliver online content and services close to ISPs for the benefit of the end user's online experience. **These investments improve user experience, reduce latency, and allow for remote working and learning.** Contrary to the argument, investments in heavy infrastructure projects, such as submarine cables and optimisation of traffic by CAPs across different internet exchange points, have materially benefitted ISPs and TSPs as they no longer need to pay transit and peering costs from the CAP's origin country. Atop this, the investments made by CAPs in maintaining optimal caches (at core/metro/aggregation nodes) reduce strain on the network provider's servers and, in effect, reduces costs for the network operator. **Studies estimate that these investments save up to USD 5-6.4 Billion annually for network operators globally.**²⁷

²⁵ Abecassis, D. et al.,(2022). *The Impact of Tech Companies' Network Investment on the Economics of Broadband ISPs. Investment on the Economics of Broadband ISPs*. Analysys Mason. Retrieved on May 12, 2023 from <https://www.analysismason.com/contentassets/b891ca583e084468baa0b829ced38799/main-report---infra-investment-2022.pdf>

²⁶ Abecassis, D. et al.(2022). *The Impact of Tech Companies' Network Investment on the Economics of Broadband ISPs. Investment on the Economics of Broadband ISPs*. Analysys Mason. Retrieved on May 12, 2023 from <https://www.analysismason.com/contentassets/b891ca583e084468baa0b829ced38799/main-report---infra-investment-2022.pdf>

²⁷ Abecassis, D., Kende, M., Osman, S., Spence, R., Choi, N.,(2022). *The Impact of Tech Companies' Network Investment on the Economics of Broadband ISPs*. Analysys Mason. Retrieved on May 12, 2023 from <https://www.analysismason.com/contentassets/b891ca583e084468baa0b829ced38799/main-report---infra-investment-2022.pdf>

- **Potential of Over Regulation:** Imposing additional regulations may not only be unnecessary but could also negatively impact the spontaneous initiatives and partnerships that have been driving the growth of both sectors. Moreover, it might create unnecessary bureaucratic hurdles that could slow down the rapid pace of innovation and development in the digital space.
- **Economic Impacts:** A singular framework might introduce new costs for OTTs and TSPs as they adapt to comply with the regulations. These costs might be passed on to the consumer, making internet-based services more expensive. Furthermore, both TSPs and OTTs would need to invest resources in understanding, implementing, and adhering to the new regulatory framework. This diversion of resources might take away from other productive and innovative ventures.
- **Barrier to Entry:** New entrants to the OTT market might find it harder to establish themselves if they have to navigate complex collaboration regulations from the outset. This could reduce competition and innovation in the OTT space.
- **International Jurisdiction Issues:** OTT platforms often operate across multiple countries, whereas TSPs are usually restricted to specific regions or nations. A singular regulatory framework in one country could create complications for OTTs that serve a global audience.
- **Additional Cost of Compliance:** India is witnessing a dynamic change in the regulatory landscape of the internet ecosystem. Along with sectoral laws that continue to evolve, Digital Personal Data Protection Act, 2023 has recently been notified and Digital India Act is in its public consultation and drafting stage. Further, the Draft Indian Telecommunication Bill, 2022 which seeks to regulate the internet and telecommunication services under an umbrella law also seems to have received the cabinet approval. There are multiple regulations that will be implemented in the coming days which will come with additional cost for the internet businesses.

At the global level, apart from South Korea's Sender Party Network Pays model which has been heavily criticised, the Body of European Regulators for Electronic Communications ('BEREC') has in the past rejected proposals by the European Telecommunications Network Operators Association ('ETNO') that requested a network interconnection fee as is observed under the SPNP model stating *"If 'bill & keep' were to be replaced by SPNP then the ISP providing access could exploit the physical bottleneck for traffic exchange and derive monopoly profits, requiring regulatory intervention."*²⁸

²⁸ Body of European Regulators for Electronic Communications. (2020, November 14). *BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines* [Press Release]. Retrieved on May 17, 2023 from

Recently, the debate was reinvigorated by the statements made by Thierry Breton, a Member of the European Parliament (MEP) and the EU commissioner for Internal Markets, over the gains made by American businesses globally in the internet services ecosystem.²⁹ However, Upon criticism³⁰ from policy experts and civil society, the commissioner also publicly assured³¹ that any policy developments to be made with regard to network usage fee would be in line with the EU's Declaration of Digital Rights and Principles³² and Net Neutrality protected under the Open Internet Regulation.

The proposal to consider an SPNP model has met with widespread resistance and cautionary interjections across the EU. Institutions such as the European Consumer Organisation³³, Europe's Mobile Virtual Network Operators (MVNO)³⁴ and the European Association for Commercial Television and Video on Demand (ACT)³⁵, amongst others, have publicly opposed the proposal and asked for careful consideration of impacts that such a transition will have for consumers and the internet as a whole. The European Consumer Organisation stated in its opposition that *“for consumers in particular, the risks or potential disadvantages of establishing measures such an SPNP system would range from a potential distortion of competition on the telecom market, negatively impacting the diversity of products, prices and performance, to the potential impacts on net neutrality, which could undermine the open and free access to the Internet as consumers*

https://www.berec.europa.eu/sites/default/files/files/document_register_store/2012/11/BoR%2812%29120rev.1_BE_REC_Statement_on_ITR_2012.11.14.pdf

²⁹ Dumoulin, S. & Perrotte, D. *Bruxelles veut faire payer les réseaux télécoms aux Gafam* Les Echos. Retrieved on May 15, 2023 from

<https://www.lesechos.fr/tech-medias/hightech/bruxelles-veut-taxer-les-gafam-pour-financer-les-reseaux-telecoms-1404614>

³⁰ Komaitis, K., Park, K. (2022, November 22) *The Global Trend That Could Kill The Internet: Sender Party Network Pays* Tech Dirt. Retrieved on May 20, 2023 from

<https://www.techdirt.com/2022/11/22/the-global-trend-that-could-kill-the-internet-sender-party-network-pays/>

³¹ Vestager, M., & Breton, T. (2023, January 10). *Reply to letter of 5 October 2022 from 29 experts and academics [Letter to Komaitis, K.]*. Retrieved from

https://www.komaitis.org/uploads/4/7/0/1/4701503/reply_to_letter_of_5_october_2022_from_29_experts_and_academics.pdf

³² European Commission (2023, February 7) *European Declaration on Digital Rights and Principles* [Press release]. Retrieved on May 17, 2023 from

<https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles#:~:text=The%20Declaration%20on%20Digital%20Rights%20and%20Principles%20presents%20the%20EU's,version%20of%20the%20Declaration%20available.>

³³ BEUC The European Consumer Organization (2022) *Connectivity Infrastructure and the Open Internet*. Retrieved on May 17, 2023 from

https://www.beuc.eu/sites/default/files/2022-09/BEUC-X-2022-096_Connectivity_Infrastructure-and-the_open_internet.pdf

³⁴ MVNO Europe. (2022). *Network Investment Contributions*. Retrieved on May 19, 2023 from

<http://mvnoeurope.eu/wp-content/uploads/MVNO-Europe-Position-on-contributions-to-network-investment-3008.pdf>

³⁵ Association of Commercial Television (2023, July 8) *TV & VoD statement on network fees [Press release]*. Retrieved on May 17, 2023 from

<https://www.acte.be/publication/tv-vod-statement-on-network-fees/>

*know it today.*³⁶

In a recent meeting with telecom ministers from across the Union, 18 countries either outrightly rejected the levy or requested an impact assessment of such a policy change from the EU Industry chief, Thierry Breton. The reasons behind such rejection included the absence of an investment shortfall, potential breach of net neutrality, a lack of adequate analysis of such policy changes and the general apprehension that added costs upon the application layer companies will likely be shifted onto the end consumer.³⁷

³⁶ Komaitis, K., Park, K. (2022). *The Global Trend That Could Kill The Internet: Sender Party Network Pays*. *Tech Dirt*. Retrieved on May 16, 2023 from

<https://www.techdirt.com/2022/11/22/the-global-trend-that-could-kill-the-internet-sender-party-network-pays/>

³⁷ Chee, F.Y. (2023 June 3) *Majority of EU countries against network fee levy on Big Tech, sources say* Reuters. Retrieved on June 13, 2023 from

<https://www.reuters.com/business/media-telecom/majority-eu-countries-against-network-fee-levy-big-tech-sources-say-2023-06-02/>

III. Issues Related to Selective Banning of OTT Services

Q10. What are the technical challenges in selective banning of specific OTT services and websites in specific regions of the country for a specific period? Please elaborate your response and suggest technical solutions to mitigate the challenges.

Answer:

OTT services have become integral in today's digital world, supporting activities like remote work, education, and business. Suggesting a selective ban on these platforms can cause considerable disruption and raise various technical, legal, and ethical concerns.

A. The technical limitations associated with selective banning

OTT applications can be restricted either by the OTT platforms themselves or by telecommunications entities. To enforce a localised block, an OTT platform must determine the user's location, typically derived from GPS or Cell ID data. However, both methods present significant challenges. Not all devices are equipped with GPS. Even devices that have GPS, necessitate user consent for access. Mandating GPS data access, potentially through government directives, raises privacy concerns.³⁸ Continuous location tracking might intrude on individual privacy, prompting some users to discontinue the usage of their devices. Consequently, if a Triangulation method of locating users is utilised, the same could constitute unwarranted surveillance and be in breach of the proportionality principle espoused in the Puttaswamy judgement. Moreover, Cell ID data is predominantly held by network operators, safeguarded from application providers due to privacy considerations.³⁹ As a result, location-based blocking by OTT platforms is impractical.

Furthermore, OTT providers have the option of using IP addresses to block access. However, this requires pinpointing the user's precise IP in a given locality. With tools like VPNs and proxy servers at users' disposal, they can easily mask their IP addresses.⁴⁰ Consequently, the malicious actors intending to skirt around the restrictions might succeed, while legitimate users would inadvertently bear the brunt of these measures.

³⁸ GPS Location Privacy, *Official U.S. government information about the Global Positioning System (GPS) and related topics*, GPS Government. Retrieved on 31 August 2023 from: <https://www.gps.gov/policy/privacy/>

³⁹ Siddharth Prakash Rao, Dr Silke Holtmanns, Dr Ian Oliver & Dr Tuomas Aura, *We Know Where You Are*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Retrieved on 31 August 2023 from" <https://ccdcoc.org/uploads/2018/10/Art-17-We-Know-Where-You-Are.pdf>

⁴⁰ Swamy, K. K., Teakumalla, S., Vemula, D., Patil, S. R., & Deepika, P. (2023). *Detection of IP Masking Using Whois*. *Turkish Journal of Computer and Mathematics Education*, 14(03), 115-124.

B. The counterproductive nature of selective banning

Restricting particular OTT platforms can detrimentally affect users dependent on them for essential services such as healthcare, education, or business functions.⁴¹ These limitations can hinder users from engaging with their OTT platform of choice for legitimate purposes. Historical trends indicate that users, when confronted with bans on their preferred platforms, often migrate to alternatives. In scenarios where a dominant OTT platform faces restrictions, there is a propensity for users to transition to lesser known niche platforms. This would mean that the banning will not be effective in stopping online misinformation or other illegal actions, which are often cited as reasons for such bans. Further, if people shift to lesser-known OTT platforms, law enforcement agencies will struggle to interact with these platforms, as they might not meet compliance requirements like having a Grievance Officer or Compliance Officer.

Another reason that is important for consideration is that the rise of VPN services can bypass such bans. For instance, when Russia blocked Facebook and Instagram, VPN usage in the country spiked.⁴²

C. Fundamental Rights and Other Underlying Legal Concerns

OTT services have seamlessly integrated into daily routines, serving not only as communication channels but also as platforms for a range of other crucial activities, including small business operations. Limiting access to such platforms might infringe upon fundamental rights, specifically those under Article 19(1)(a) and Article 19(1)(g) of the Constitution. Article 19(1)(a) guarantees every citizen the right to freedom of speech and expression. Many OTT platforms are now conduits for this expression, be it through content creation, sharing, or consumption. Curtailing access could stifle this expression. Simultaneously, Article 19(1)(g) ensures the right to practise any profession or carry on any occupation, trade, or business. In the digital age, countless small businesses rely on OTT services, either as their primary operational platform or as a critical component of their business model. Restricting access to these services can thus impede their right to conduct business, as established by the Constitution.

Before implementing such bans, it is crucial to consider the principle of proportionality.⁴³ This principle provides that any curtailment of fundamental rights should only occur if there is a valid objective, the applied restrictions are minimal and necessary, and no better alternative exists. Currently, there is ambiguity whether selectively banning OTT services is the most effective

⁴¹ Office of the High Commissioner, United Nations Human Rights (2011 August 10). *Using Social Media to Promote Human Rights*. Retrieved on 31 August 2023 from:

<https://www.ohchr.org/en/stories/2011/08/using-social-media-promote-human-rights>

⁴² Anthony Faiola. (2022 May 6), How millions of Russians are tearing holes in the Digital Iron Curtain. *The Washington Post*. Retrieved on 31 August 2023 from:

<https://www.washingtonpost.com/world/2022/05/06/russia-vpn-putin-censorship-disinformation/>

⁴³ *Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1.*

approach for countering illegal and harmful online content or for upholding public order during times of public unrest. Accordingly, given the inadequacy of data to substantiate the proportionality principle in this situation, the proposal for selective banning should not be pursued.

D. Concerns with URL level blocking

In the Parliamentary Standing Committee on Communications and Information Technology's 26th report on "Suspension of Telecom Services/Internet and its Impact," presented by the Department of Telecommunications, it was highlighted that selectively blocking services hosted on cloud platforms poses challenges.⁴⁴ These services, due to their decentralised nature, function across various locations and countries, and can easily migrate between services. On the contrary, websites with static URLs can be more straightforwardly blocked owing to their consistent domain names and associated IP addresses. It is certainly easier to selectively ban websites given their fixed domains and URLs, which makes their IP addresses easy to identify and block. However, it is important to note that users may attempt to circumvent such a ban, for example, by relying on VPN services available for use in India.⁴⁵

E. Concerns with Application level blocking

- **OTT level blocking**

For OTT service providers to block content in specific geographic regions, they would need to determine the exact location of their users. These providers might not always have this information readily available due to the user's privacy preferences. Furthermore, accessing such location data may not be consistent with the overarching judicially recognised privacy principles⁴⁶ as well as the norms of the new Digital Personal Data Protection Act, 2023⁴⁷.

- **TSP-level blocking**

TSPs might also try to selectively ban OTT applications by targeting the IP addresses linked to the servers used by OTT service providers. However, this endeavour is also replete with difficulties, such as the reluctance of an OTT service provider to disclose its IP addresses to TSPs, fearing the consequent risk of cybersecurity breaches.

⁴⁴ Twenty-sixth Report Standing Committee on Communications and Information Technology (17th Lok Sabha) on 'Suspension of telecom services/internet and its impact' relating to the Ministry of Communications (Department of Telecommunications). Retrieved on August 31 August 2023 from:

https://eparlib.nic.in/bitstream/123456789/820699/1/17_Communications_and_Information_Technology_26.pdf

⁴⁵ Sunaina Chadha. (2022 May 12), Explained: What the new VPN rules means for internet users in India. *The Times of India*. Retrieved on 31 August 2023 from:

<https://timesofindia.indiatimes.com/business/india-business/explained-what-the-new-vpn-rules-means-for-internet-users-in-india/articleshow/91510719.cms>

⁴⁶ Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1.

⁴⁷ Digital Data Protection Act, 2023, Act No. 23 of 2023, Parliament of India.

- **Instances of over-blocking**

As highlighted by the Department of Telecommunications, OTT services usually operate from the cloud, possessing dynamic IP addresses. Accordingly, when TSPs may attempt to selectively block based on these dynamic IPs, they may inadvertently block other OTT services sharing the same cloud and IP address.

Utilising deep-packet inspection offers a solution to prevent such over-blocking, but this approach comes with its own set of significant legal challenges.⁴⁸ To effectively implement this, TSPs would need to delve into every piece of data transmitted over the internet to pinpoint the exact OTT service to block. This extensive probing and interception of online data packets not only presents logistical challenges but also raises crucial concerns about privacy, *chilling effect* on free speech and undermining the principles of net neutrality.

Q11. Whether there is a need to put in place a regulatory framework for selective banning of OTT services under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 or any other law, in force? Please provide a detailed response with justification.

Answer:

Based on our earlier response to Question 10, we recommend against the implementation of a framework that enables selective banning. Consequently, introducing any supplementary framework for selective bans under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 or any other existing or upcoming legislation is unnecessary and disproportionate at this juncture. The current legal provisions within the IT Act sufficiently cater to the requirements for regulating online content and OTT service blocking.

For instance, Section 69A of the IT Act⁴⁹, read alongside Information Technology. (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009⁵⁰, provides for the blocking of online content (encompassing entire OTT platforms) based on reasons such as the sovereignty and integrity of India, national security, and public order. The Central Government has used Section 69A on multiple occasions to block several OTT platforms citing national security reasons. Additionally, Section 79 of the IT Act⁵¹, read alongside Rule 3 of the IT Rules, 2021⁵², permits the restriction of online content based on specific criteria.

⁴⁸ Mayan Perel. (2020). Digital Remedies. *Berkeley Technology Law Journal*. 35(1), 25.

⁴⁹ Section 69A, Information and Technology Act 2000, Act No. 21 of 2000. Parliament of India.

⁵⁰ Rule 9, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, G.S.R. 781 (E).

⁵¹ Section 79, Information and Technology Act 2000, Act No. 21 of 2000. Parliament of India.

⁵² Rule 3, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

While there are some principle level and procedural concerns under the existing Section 69-A framework as well as the IT Rules, 2021 that needs to be addressed in the upcoming Digital India Act, there is certainly no need for another concurrent blocking/ banning framework that might lead to regulatory disharmony and compliance uncertainty.

Answers to Q.12 - Q.14.

We recommend against the implementation of additional regulations for OTT services or the selective banning of OTT platforms or websites, as elaborated in Questions 10 and 11. Accordingly, we do not have any further inputs to provide to these questions.