Asia Internet Coalition (AIC) Industry Submission

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

---

1 Sept 2023

To,

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

Dear Mr. Trivedi,

On behalf of the Asia Internet Coalition (AIC) and its members, 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 ("**CP**"). AIC is an industry association comprising leading internet and technology companies. We seek to promote technology and policy issues in the Asian region, and we are fully committed to the cause of a safe and open internet.

Notably, we would like to stress on the following aspects and raise our concerns that by regulating OTTs, TRAI risks the following:

- A mandatory / mandated collaborative framework between OTT service providers and licensed TSPs may lead to the creation of a system where TSPs can demand compensation from OTT service providers in the form of revenue sharing or network usage fees. This will **impact net neutrality** and consumer well-being in the long run. More importantly, a revenue sharing or network usage fees model will likely violate the principle of net neutrality. For example, if TSPs are permitted to charge different rates to different OTT services (which could be based on a variety of factors such as the existing relationship with an OTT service, or whether these rates are contingent depending on the popularity of such service), then the principle of net neutrality becomes violated. TSPs may also create revenue sharing exemptions for their own OTT services (especially given that most TSPs have ventured into the OTT space as well) and this can lead to concerns under both the principle of net neutrality, as well as competition law.
- Any further regulation would **harm market competition** in the digital services industry. It will adversely impact business operations of OTT service providers in India in the event onerous regulations that traditionally have always been applied to the telecom sector in India are also made applicable to the OTT services sector. Particularly, subjecting OTT services to any form of licencing will likely deter future investments in the sector. It may also lead to a scenario where OTT service providers pass on the costs arising from such licencing regime to their users. Given that the internet is meant to be free and open, the possibility that certain users may ultimately no longer be able to afford accessing critical OTT services is a cause for concern.

The CP refers to policy initiatives undertaken by organisations such as the ITU on exploring the need to introduce a collaborative framework between TSPs and OTT service providers. As part of this, the ITU has recommended that a collaborative framework that would promote competition, consumer protection, consumer benefits, innovation, investment, infrastructure development, etc. in relation to the global growth of OTT platforms. The current economic environment and existing free market practices promote these aspects. Accordingly, there is **no need for introducing a collaborative framework between OTT service providers and licenced TSPs.** In fact, we note that OTT service providers have invested in the development of passive internet infrastructure across the globe and have undertaken connectivity projects in India to ensure better quality internet services. OTT services have to maintain minimum quality of service in order to survive a market with extremely high competition. **A drop in quality in one OTT service can trigger users to switch to other competing OTT services**. In order to pre-empt such a situation, we understand that OTT service providers strive to ensure that their users get the best quality services. Thus, this free-market regime is sufficient for the time being and there should be no requirement for OTT service providers to be bound by pre-determined quality of service requirements (an aspect that will also hinder their ability to frequently innovate and introduce new features for their services).

Lastly, the TRAI in the CP has recognised various definitions of OTT service which highlight the technical nature of such services. For instance, the Office of Communications, United Kingdom defines OTT services as ""over the top" of an existing data network connection". The Commonwealth Telecommunication Organization in its report on 'Over The Top (OTT) Applications & Internet Value Chain' defines it as a service/content/application that is provided to the end-user "over the public internet". The **Body of European Regulators for Electronic Communications ("BEREC") adopted a similar definition for OTT services in its 'Report on OTT Services'**.

Given the context above, as an industry stakeholder, we take this opportunity to provide our **detailed comments and recommendations on the CP**, for TRAI's sincere consideration. Our observations have been annexed in a question-answer format in the following sections:

- **PART A: Issues Related to regulatory Mechanisms for OTT Communication Services**
- **PART B: Issues Related to Selective Banning of OTT Services**

As an industry stakeholder, we take this opportunity to provide our inputs and comments on the CP. Our observations have been annexed in a question-answer format. We hope to be of assistance to the TRAI in identifying the challenges that arise vis-à-vis regulating over-the-top ("**OTT**") services.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Thank you for your time and consideration. We would also be happy to offer our inputs and insights directly through meetings and discussions with the relevant authorities.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed comments and recommendations with responses to Questions

PART A: Issues Related to regulatory Mechanisms for OTT Communication Services

Q1. What should be the definition of over-the-top (OTT) services? Kindly provide a detailed response with justification.

At the outset, OTT services operate on the application layer to transfer data or content to consumers, whereas telecom services operate on the network layer, which drives the operation of the internet. The separation between these layers was recognised by the TRAI in its 2017 Report titled 'Recommendations on Regulatory Framework for Internet Telephony' with respect to internet telephony services.[1]

The TRAI in the CP has recognised various definitions of OTT service which highlight the technical nature of such services. For instance, the Office of Communications, United Kingdom defines OTT services as ""over the top" of an existing data network connection".[2] The Commonwealth Telecommunication Organization in its report on 'Over The Top (OTT) Applications & Internet Value Chain' defines it as a service/content/application that is provided to the end-user "over the public internet".[3] The Body of European Regulators for Electronic Communications ("**BEREC**") adopted a similar definition for OTT services in its 'Report on OTT Services'.[4]

In light of this, we recommend the following definition for the term 'OTT services':

Recommendation: An OTT service is a type of service that can be accessed by the end user through the public internet or over the top of an existing network connection.

Q2. What could be the reasonable classification of OTT services based on an intelligible differentia? Please provide a list of the categories of OTT services based on such classification. Kindly provide a detailed response with justification.

OTT is a medium through which a service is provided and does not indicate the nature of the service itself. Various OTT services offer multiple functionalities to the user in an effort to improve user convenience and enable a seamless user experience, for instance, think of a ride hailing platform that not only enables users to book and pay for taxis, but also message or speak with taxi drivers.

Accordingly, we believe that there is no requirement to identify sub-categories of OTT services at this stage of the consultation process, and our comments in this document are focused on OTT services as a whole.

---

[1]Please note that TRAI Recommendations on Regulatory Framework for Internet Telephony dated October 24, 2017, stated the following: "*The separation of network and service layers of telecom service offerings is the natural progression of the technological changes in this domain. It is now possible to separate provision of service contents, configuration and modification of service attributes regardless of the network catering to such service."*

[2]The Office of Communications, United Kingdom, Mobile Call Termination Market Review 2015-18, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0025/74257/annex_15_glossary.pdf.

[3] Commonwealth Telecommunication Organization, Report on 'Over The Top (OTT) Applications & Internet Value Chain' 2020, available at https://cto.int/wp-content/uploads/2020/05/CTO-OTT-REPORT-2020.pdf.

[4] Body of European Regulators for Electronic Communications, Report on OTT Services, available at https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-ott-services.

Q3. What should be the definition of OTT communication services? Please provide a list of features which may comprehensively characterize OTT communication services. Kindly provide a detailed response with justification.

We reiterate our response to Question 2, i.e., we believe that there is no need to, at this stage, identify the different types of OTT services that exist, and as a corollary, there is also no requirement to define what is an 'OTT communication service'. That said, we would like to focus our response to this Question 3 on differentiating between OTT services and traditional telecom services.

As noted above, it is important to acknowledge the 'over the top' nature of OTT services, and the fact that OTT services and telecom services cannot be regarded as being substitutable in nature. To elaborate:

- TSPs operate on the network layer, where they provide network connectivity to subscribers and the like. OTT service providers rely on the same to provide online services 'over' this very network connectivity provided by TSPs.
- Further, consumers do not view telecom services and OTT services as substitutable services. In fact, OTT services provide a range of different services (ranging from social media to online shopping, and food delivery to document sharing) which are not provided by traditional telecom services. We believe that consumers tend to view OTT services as an offering they can access in addition to traditional telecom services. That is, consumers may choose to use both of these services together or only use legacy telecom services. Therefore, functionally, OTT services and telecom services are not comparable services.
- TSPs also play the role of 'gatekeepers' – (a) since they provide network connectivity required by OTT service providers to offer their services to the end-user, and (b) since the end-user relies on this very network connectivity to access OTT services. That is, users need to purchase a network connection or data packet first in order to access OTT services. Thus, it is clear that OTT service providers are depended on TSPs and not the other way around.
- Due to the nature of their operations, TSPs have access to critical resources (that are owned and licensed by the State). They have the right to acquire spectrum from the Government, interconnect with the Public Switched Telephone Network ("**PSTN**"), build network infrastructure, etc. Unlike TSPs, OTT service providers, as such, have no control over the manner in which deployment and development of network infrastructure takes place.

Q4. What could be the reasonable classification of OTT communication services based on an intelligible differentia? Please provide a list of the categories of OTT communication services based on such classification. Kindly provide a detailed response with justification.

At the outset, please note that at this stage, we do not believe it is necessary to create sub-categories of OTT services (including sub-categories of OTT communication services). Accordingly, we have limited our responses to the questions posed by the CP vis-à-vis OTT services as a whole.

Q5. Please provide your views on the following aspects of OTT communication services vis-à-vis licensed telecommunication services in India:

(a) Regulatory aspects;
(b) Economic aspects;
(c) Security aspects;
(d) Privacy aspects

(e) Safety aspects;
(f) Quality of service aspects;
(g) Consumer grievance redressal aspects; and
(h) Any other aspects (please specify).

Kindly provide a detailed response with justification.

In the table below, we have, among other things, highlighted the various sectoral laws and regulations in India which govern the functioning of OTT services. We believe that these are sufficient for the time being and any attempt to bring additional regulation on any of these aspects will severely impact the ease of doing business in the country and generally give rise to business uncertainty in the OTT sector.

S. No.	Aspect under consideration	Observations and Recommendations
1.	Regulatory Aspects	<u>Demand by TSPs for regulation of OTT communication services:</u> We note that TSPs have long demanded for the regulation of OTT services in a like manner on the principle of 'same service, same rules' and in order to create a supposed 'level playing field'. However, we reiterate that there are substantial differences in the nature of services provided by OTT service providers and TSPs. Below is an overview of the key technical and operational differences between these players and on account of which they ought to be regulated differently- ● TSPs operate on the network layer to provide data and telecom connectivity, whereas OTT service providers operate on the application layer to provide services to their users. ● TSPs operate in a restricted market where only limited players have access to certain rights (such as the right to acquire spectrum, obtain numbering resources and interconnect with the PSTN). OTT service providers do not have access to these rights, and as such, cannot be subject to regulations designed keeping the operations and features of telecom services in mind. ● Further, unlike the telecom market, there exist lower barriers to entry for digital services, which has been a foundational feature enabling far more rapid innovation and growth for the sector, and greater consumer choice (e.g. by allowing consumers to switch between competing applications, such as through multi-homing) <u>Existing regulations for OTT service providers:</u> OTT service providers are already subject to regulation under the Information Technology Act, 2000 ("**IT Act**") and the rules and regulations issued thereunder. These include the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**Rules on Data**

S. No.	Aspect under consideration	Observations and Recommendations
		Privacy and Security Practices"), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**Rules for Interception**"), the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("**Rules for Blocking**"), the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**Cyber-security Rules**"), the Cyber-security Directions of April 2022 issued under Section 70B(6) of the IT Act ("**Cyber-security Directions**"), and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021) ("**Intermediary Rules**"). They will also be subject to the requirements under the upcoming Digital Personal Data Protection Bill, 2023 ("**DPDP Bill**") as well as the proposed Digital India Act ("**DIA**") -[5] based on public statements made by the Central Government. Thus, there is no need to consider the introduction of additional or incremental regulations for OTT services. The same will only lead to unnecessary regulatory overlap and cause business uncertainty in the country.
2.	Economic Aspects	<u>OTT services' immense economic contributions:</u> There is a view within the telecom industry that OTT services 'free ride' over the network services provided by TSPs and should compensate them for the same. However, this viewpoint disregards the fact that OTT services have positively contributed to the revenues generated by TSPs. To elaborate, the growth of the digital economy has led to an increase in the number of users who have internet access. This in turn has led to an increase in the demand for online applications and services generated by OTT service providers. In order to access such services, users have to purchase data from TSPs – thus contributing to their revenues. This analysis has been supported by the Broadband India Forum's recent report on the 'Economic Value of the App Economy in India' where it stated, "Besides the **direct effect of the app economy on the GDP, there are spill-over effects in the supply industries (computer hardware, telecommunication and ICT services**)…An increase in sales in the App Economy not only gives

[5]Please see 'Presentation made during the Digital India Dialogues on the proposed Digital India Act on 9th March in Bengaluru, Karnataka', available at https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf and 'MoS Rajeev Chandrasekhar holds Digital India Dialogues in Mumbai on the Principles of the Digital India Act', available at https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1926711

S. No.	Aspect under consideration	Observations and Recommendations
		rise to an increase in GDP but also creates a multiplier effect through indirect and induced effects…."[6] The following statistics lend credence to our position that TSPs have indeed gained from an increase in data usage and consumption of online services. ● From 2012 to 2022, the monthly average revenue per user for wireless services in India grew by about 44%. ● From 2014 to 2022, the volume of monthly usage of wireless data has grown by about 156 times. ● From 2014-2022, the average revenue from data usage per wireless subscriber per month increased about 5.6 times. Lastly, BEREC in its October 2022 report 'BEREC preliminary assessment of the underlying assumptions of payments from large CAPs [content and information providers] to ISPs'[7] – while discussing the need to introduce a compensation mechanism between OTT services and ISPs - highlighted the following: "10. CAPs and ISPs are mutually dependent on each other. 11. The demand from ISPs customers for content drives demand for broadband access. 12. Availability of broadband access drives demand for content. 13. There is no evidence of "free-riding."
3.	Security aspects	In terms of 'security', especially cyber security, OTT services are subject to various security requirements present under various regulations. Accordingly, there is no need for further regulation on this aspect. A brief summary of these regulations is as follows: <u>Cyber-security Rules:</u> The Indian Computer Emergency Response Team ("**CERT-In**") is the national nodal body to ensure cyber security. It oversees the Cyber-security Rules and Cyber-security Directions. A wide range of entities including OTT service providers are subject to various cyber-security related obligations in this regard. For example, OTT service provider need to report any incidence of specific cyber security incidents to the CERT-In, as well as designate a point of contact to interface and communicate with the CERT-In. <u>IT Act and rules and regulations thereunder:</u>

[6]Broadband India Forum, Report on Economic Value of the App Economy in India, June 2023, available at https://broadbandindiaforum.in/wp-content/uploads/2023/06/Research-paper-on-THE-ECONOMIC-VALUE-OF-THE-APP-ECONOMY-IN-INDIA.pdf.

[7] BEREC, Preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs, October 7, 2022, available at https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%20%2822%29%20137%20BEREC_preliminary-assessment-payments-CAPs-to-ISPs_0.pdf.

S. No.	Aspect under consideration	Observations and Recommendations
		All body corporates (which will include OTT service providers) are required to comply with the SPDI Rules if they are dealing with or processing personal information ("**PI**") and sensitive personal data or information ("**SPDI**"). Under Section 43A of the IT Act, "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected." The Rules for Data Privacy and Security Practices issued under Section 43A stipulate the various reasonable security practices and procedures that an entity (such as an OTT service provider) should implement. This is, of course, in addition to the fact that the upcoming DPDP Bill will also likely require entities such as OTT service providers to implement security practices in the interests of protecting the PI or SPDI they are processing. <u>Content blocking and interception:</u> Under the IT Act, the State is enabled to undertake measures relating to content regulation on the grounds of, among other things, national security. For instance – ● Section 69[8] read with the Rules for Interception empower the Government to issue interception, monitoring, decryption directions vis-à-vis any information generated, transmitted, received or stored in any computer resource. ● Section 69A[9] read with the Rules for Blocking empower the Government to issue blocking orders vis-à-vis any information generated, transmitted, received, or stored in any computer resource; and ● Section 69B[10] read with the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 ("**Rules for Monitoring Traffic**")

[8]Intermediaries or persons in-charge of a computer resource are required to extend all facilities and technical assistance on receiving directions from Government agencies under Section 69 of IT Act for interception, monitoring, or decryption of any information through a computer resource. The procedure and safeguards subject to which such interception, monitoring or decryption may be carried out are prescribed under the Rules for Interception.

[9]Intermediaries are required to implement orders issued by the Government under Section 69A of IT Act regarding blocking of any information for public access. The procedure and safeguards governing such blocking orders are prescribed under the Rules for Blocking.

[10]Intermediaries or persons in-charge of a computer resource are required to extend all facilities and technical assistance to authorized Government agencies to monitor and collect traffic data / information for cyber security purposes on receiving directions under Section 69B of the IT Act. The applicable procedure and safeguards are prescribed under the Rules for Monitoring Traffic.

S. No.	Aspect under consideration	Observations and Recommendations
		empower the Government to issue directions to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource for cyber-security purposes.
4.	Privacy Aspects	The existing framework under the Rules for Data Privacy and Security Practices subject body corporates (such as OTT service providers) to various privacy related compliances. These include- obtaining informed consent for the collection and use of SPDI, designating a grievance officer for grievance redressal within the timeframe specified, developing a clear and easily accessible privacy policy for processing of PI or SPDI, amongst others. Once the DPDP Bill becomes law, these obligations would get even more heightened and stringent, and would require a higher degree of compliance on part of OTT service providers.
5.	Safety aspects	At the outset, the general objective behind the CERT-In framework (i.e., the Cyber-security Rules and Cyber-security Directions) is to ensure that users are safe from cyber-threats. Similarly, Section 43A of the IT Act read with the Data Privacy Laws aim to ensure that a user's PI and SPDI is processed in a secure manner and adequately protected. In addition, the DIA will also likely contain safety-related requirements. Over and above this, OTT service providers have undertaken their own initiative to secure user safety on their online platforms. This includes methods such as, two-step verification (for signing up / logging in), the option to block or report other user accounts, the ability for users to implement privacy controls (such as limiting the visibility of their profile pictures), and in-app solutions to reduce the incidence of spam and fake news. Lastly, we note that OTT service providers have entered into voluntary arrangements with regulatory authorities to de-register or block accounts of users who have obtained mobile numbers by fraudulent means.[11]
6.	Quality of service aspects	OTT services have to maintain minimum quality of service in order to survive a market with extremely high competition. A drop in quality in one OTT service can trigger users to switch to other competing OTT services. In order to pre-empt such a situation, we

[11]For example, 'WhatsApp cooperated in blocking numbers we flagged using AI: IT Minister', available at https://indianexpress.com/article/technology/tech-news-technology/whatsapp-cooperated-in-blocking-numbers-we-flagged-using-ai-it-minister-8613273/; WhatsApp to axe numbers flagged fraud on DoT's portal, available at https://economictimes.indiatimes.com/tech/technology/whatsapp-to-axe-numbers-flagged-fraud-on-dots-portal/articleshow/100285792.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

S. No.	Aspect under consideration	Observations and Recommendations
		understand that OTT service providers strive to ensure that their users ger the best quality services. Thus, this free-market regime is sufficient for the time being and there should be no requirement for OTT service providers to be bound by pre-determined quality of service requirements (an aspect that will also hinder their ability to frequently innovate and introduce new features for their services).
7.	Consumer grievance redressal aspects	OTT service providers (which are intermediaries under the IT Act) are already subject to grievance redressal requirements under the Intermediary Rules. In this regard, they are required to follow due diligence requirements such as, publishing the contact information of the grievance officer and redressal of complaints within prescribed timelines, etc. Under the consumer protection framework, they are subject to the grievance redressal provisions under the Consumer Protection Act, 2019 and its rules to the extent they provide paid online or electronic services. Similarly, Section 43A read with the Rules for Data Privacy and Security Practices also require OTT service providers to appoint a grievance officer to resolve user grievances vis-à-vis their PI or SPDI.

Q6. Whether there is a need to bring OTT communication services under any licensing/regulatory framework to promote a competitive landscape for the benefit of consumers and service innovation? Kindly provide a detailed response with justification.

There are already existing regulatory obligations and compliances, including those in the pipeline, that regulate OTT service providers and hold them accountable. Any further regulation would harm market competition in the digital services industry due to the following reasons –

- Firstly, it will adversely impact business operations of OTT service providers in India in the event onerous regulations that traditionally have always been applied to the telecom sector in India are also made applicable to the OTT services sector. Particularly, subjecting OTT services to any form of licencing will likely deter future investments in the sector. It may also lead to a scenario where OTT service providers pass on the costs arising from such licencing regime to their users. Given that the internet is meant to be free and open, the possibility that certain users may ultimately no longer be able to afford accessing critical OTT services is a cause for concern. Additionally, a strict licensing regime would be a barrier to new, innovative entrants. Start-ups and smaller entities may not have the resources to obtain/maintain a license. This would mean Indian consumers wouldn't have access to new, innovative services that their global peers have access to, and if other countries were to enact reciprocal requirements, that would impose a barrier to Indian start-ups and entrepreneurs.

- Secondly, a licensing regime will adversely impact OTT service providers' ability to constantly innovate in the digital technologies field and generate meaningful value for their OTT services in the eyes of users. This in turn will hinder their ability to survive in a market that is characterised with high due to very low barriers of entry.

In light of the above, we reiterate that OTT services should not be subject to any additional regulation and licensing framework designed for regulating telecom services.

Q7. In case it is decided to bring OTT communication services under a licensing/ regulatory framework, what licensing/ regulatory framework(s) would be appropriate for the various classes of OTT communication services as envisaged in the question number 4 above? Specifically, what should be the provisions in the licensing/ regulatory framework(s) for OTT Communication services in respect of the following aspects:

(a) lawful interception;
(b) privacy and security;
(c) emergency services;
(d) unsolicited commercial communication;
(e) customer verification;
(f) quality of service;
(g) consumer grievance redressal;
(h) eligibility conditions;
(i) financial conditions (such as application processing fee, entry fee, license fee, bank guarantees etc.); and
(j) any other aspects (please specify).

Kindly provide a detailed response in respect of each class of OTT communication services with justification.

At the outset, we have highlighted in our response to Question 6 above that there is no need to introduce any licensing framework for OTT services. It will have an adverse impact on the competitive landscape of the industry, and hinder initiatives to pursue innovation in the digital technologies field. With this background, we have provided our inputs to the various aspects in the table below.

S. No.	Aspects under consideration	Observation and Recommendations
1.	Lawful interception	Section 69 read with the Rules for Interception and Section 69B read with the Rules for Monitoring Traffic are sufficient in terms of empowering Governmental authorities for conducting lawful interception vis-à-vis an OTT service under specific grounds. For more details, please refer to our response in Question 5.
2.	Privacy and security	The Cyber-security Rules read with the Cyber-Security Directions, as well as the Rules for Data Privacy and Security Practices impose sufficient obligations on OTT services in terms of ensuring privacy and security of their users, data, etc. For more details, please refer to our response in Question 5.
3.	Emergency Services	TSPs are required to provide emergency or public utility services under the Unified License framework, which includes as toll-free services for police, fire, and ambulance, etc. The objective being

S. No.	Aspects under consideration	Observation and Recommendations
		that subscribers should not be hindered from accessing public emergency services, if they are unable to pay for making a phone call during times of emergency. In this regard, we would like the TRAI to note that due to various technical issues (as outlined below) OTT service providers are not best placed to offer emergency services and accordingly should not be mandated to do so- ● Most OTT services do not connect to the PSTN and do not necessarily have the technical infrastructure required to provide emergency calling services or even convey emergency announcements / messages. ● OTT service providers require internet to provide users with their services and vice versa, i.e., users need the internet to access OTT services. In light of this, OTT services should not be relied on to provide emergency messaging or calling services especially because an internet connection may not be available to a user at all points of time. ● Lastly, OTT platforms do not always have access to an individual's geo-location which may have to be accessed in order to provide emergency assistance during search and rescue operations. Mandating OTT service providers to provide emergency services would require them to rely on third party tracking services for compliance, especially in the event users do not give permission to access their locations.
4.	Unsolicited commercial communication	OTT services typically come with in-built features to report or block senders of unsolicited commercial messages and calls (to the extent they allow commercial communication on their platforms). In addition, some even provide an option for users to opt-out or unsubscribe from such services, instead of blocking a commercial number. We believe that these measures are sufficient for the time being.
5.	Customer Verification	Customer verification is an in-built feature for many OTT services. That is, verification is carried out for users looking to sign up or log-in to an OTT service by way of an OTP sent to their phone numbers or email IDs. Moreover, under the Intermediary Rules, significant social media intermediaries are subject to certain user verification requirements. That is, they have to enable users to voluntarily verify their accounts using, for example, their active India mobile number. Given that the threshold for being a significant social media intermediary is 50 lakh registered users in India, it is likely that a large number of OTT platforms that fulfill the criteria of a 'significant social media intermediary' will be subject to this requirement.

S. No.	Aspects under consideration	Observation and Recommendations
		In certain cases, we note that few OTT service providers have also entered into voluntary agreements with regulatory authorities to tackle instances where users with disconnected phone numbers are able to continue using an OTT service. In order to tackle this, OTT service providers conduct a re-verification of such numbers.
6.	Quality of service	OTT services are incentivised to maintain high quality of service on their own. For more details, please refer to the response to Question 5 above on 'quality of service aspects'.
7.	Consumer Grievance Redressal	OTT services are subject to grievance redressal requirements under extant laws. Please refer to the response to Question 5 above on 'consumer grievance redressal aspects'.
8.	Eligibility conditions	We have recommended that there is no need to introduce a new licensing or regulatory framework for OTT service providers, and hence we have not provided our inputs on this aspect.
9.	Financial Conditions	We have recommended that there is no need to introduce a new licensing or regulatory framework for OTT service providers, and hence we have not provided our inputs on this aspect.

Q8. Whether there is a need for a collaborative framework between OTT communication service providers and the licensed telecommunication service providers? If yes, what should be the provisions of such a collaborative framework? Kindly provide a detailed response with justification.

The CP refers to policy initiatives undertaken by organisations such as the ITU on exploring the need to introduce a collaborative framework between TSPs and OTT service providers. As part of this, the ITU has recommended that a collaborative framework that would promote competition, consumer protection, consumer benefits, innovation, investment, infrastructure development, etc. in relation to the global growth of OTT platforms.[12] The current economic environment and existing free market practices promote these aspects. Accordingly, there is no need for introducing a collaborative framework between OTT service providers and licenced TSPs.

- In its paper titled 'Economic impact of OTTs on national telecommunication/ICT markets', the ITU noted that "many collaborative initiatives exist between operators, development agencies and Internet companies aimed at co-investment in network infrastructure."[13] In fact, we note that OTT service providers have invested in the development of passive internet infrastructure across the globe and have undertaken connectivity projects in India to ensure better quality internet services.[14]

[12] ITU's 'Economic impact of OTTs on national telecommunication/ICT markets', available at https://www.itu.int/dms_pub/itu-d/oth/07/23/D07230000030001PDFE.pdf

[13] ITU's 'Economic impact of OTTs on national telecommunication/ICT markets', available at https://www.itu.int/dms_pub/itu-d/oth/07/23/D07230000030001PDFE.pdf

[14] For example, Meta Platforms and Google have taken various initiatives in this regard. For more information, please see https://telecominfraproject.com/facebook-partnering-to-build-the-telecom-infra-project/, and https://indianexpress.com/article/business/airtel-partners-with-meta-to-develop-undersea-cable-infra-for-high-speed-internet-8307705/, and https://cloud.google.com/blog/products/infrastructure/announcing-the-blue-and-raman-subsea-cable-systems

- A report by Analysys Mason titled 'The Impact of Tech Companies' Network Investment on The Economics of Broadband ISPs' in the context of demands made by ISPs to be compensated from OTT service providers makes the following pertinent observations:[15]

    - Substantial investments have been made by OTT service providers for hosting, transport, and delivery networks, which is alongside the investments made by ISPs and other stakeholders operating in the Internet ecosystem. The investments made by OTT service providers have been on an upward trend with the average investment made 2018 and 2021, being USD 120 billion annually.
    - The growth of the internet has been positively affected by the mutual collaboration between OTT service providers and ISPs. The same has correspondingly led to a growth in the demand for online services and broadband.

As OTT service providers continue to invest significant amounts in internet infrastructure, this improves service delivery to end users, and also provides significant cost savings to ISPs.

Q9. What could be the potential challenges arising out of the collaborative framework between OTT communication service providers and the licensed telecommunication service providers? How will it impact the aspects of net neutrality, consumer access and consumer choice etc.? What measures can be taken to address such challenges? Kindly provide a detailed response with justification.

A mandatorily collaborative framework between OTT service providers and licensed TSPs may lead to the creation of system where TSPs can demand compensation from OTT service providers in the form of revenue sharing or network usage fees. This will impact net neutrality and consumer well-being in the long run. Our concerns with this are as follows:

- <u>Incremental revenues earned by TSPs</u>

  In the event a revenue sharing or network usage fees model is introduced, TSPs will be able to seek (a) payment from users who seek to purchase data, as well as (b) payment from OTT services who rely on TSPs' network services to transmit their content or services online. We take this opportunity to highlight an observation in a report by the Analysys Mason Report, "growth in traffic has not been accompanied by corresponding increases in network costs, as significant portions of ISPs' networks are not sensitive to traffic".[16] Thus, there is no discerning need to provide TSPs with an additional source of revenue. Additionally, there is no evidence that the current system of charging users is not sufficient, nor is there evidence that "double-charging" OTT service providers for data that the user already pays for is essential to the growth of infrastructure. Prima facie, this demand from TSPs appears to be more to increase profit, and not one borne from necessity. In fact, there is nothing to prevent TSPs from directing such revenue towards their profits, rather than for the development of network connectivity infrastructure and improving their telecom services.

- <u>Violation of the principle of net neutrality</u>

  More importantly, a revenue sharing or network usage fees model will likely violate the principle of net neutrality. For example, if TSPs are permitted to charge different rates to different OTT

[15] Analysys Mason, The Impact of Tech Companies' Network Investment on the Economics of Broadband ISPs, October 2022, available at https://www.analysysmason.com/contentassets/b891ca583e084468baa0b829ced38799/main-report---infra-investment-2022.pdf.

[16] Analysys Mason, The Impact of Tech Companies' Network Investment on the Economics of Broadband ISPs, October 2022, available at https://www.analysysmason.com/contentassets/b891ca583e084468baa0b829ced38799/main-report---infra-investment-2022.pdf.

services (which could be based on a variety of factors such as the existing relationship with an OTT service, or whether these rates are contingent depending on the popularity of such service), then the principle of net neutrality becomes violated. TSPs may also create revenue sharing exemptions for their own OTT services (especially given that most TSPs have ventured into the OTT space as well) and this can lead to concerns under both the principle of net neutrality, as well as competition law.

- Reduction in investments made by OTT services

  If revenue sharing or network usage fees is implemented, OTT services may have to redirect their existing investment towards making such payments, which could have, ideally been used for improving the quality of their services or for developing passive infrastructure in the country. The collective impact of this would be on end-users who would not only miss out on high quality of services from OTT service providers, but also on good quality network connectivity that is crucial for day-to-day functioning. Moreover, there is a strong likelihood that such revenue sharing models will cause damage to the digital ecosystem, and result in several negative externalities arising as a result of the ecosystem's inhibited growth.

  In this regard, lessons should be learned from South Korea's experience, which follows a 'Sending-Party-Network-Pays' regime where TSPs are required to charge fees for data traffic they receive from one another. TSPs have, however, passed on these charges to OTT service providers. This regime has been criticised and considered as a failure because it has led to poor quality of network services, increased prices for end-users, decline in diversity of online content, and imposition of entry-barriers in the OTT sector.[17]

- Opposition from industry stakeholders:

  Even multiple industry stakeholders and think tanks – such as CUTS International and the Internet and Mobile Association of India - have raised similar concerns against introducing a revenue sharing model in India.[18]

PART B: 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.

Based on our experience working with the industry, we note that selective banning of OTT services would lead to various legal, policy and technical challenges. These are as follows:

[17]Internet Society, 'Internet Impact Brief – South Korea's Interconnection Rules', available at https://www.internetsociety.org/wp-content/uploads/2022/05/IIB-South-Korea-Interconnection-Rules-2022.pdf; WIK-Consult Report, 'Competitive conditions on transit and peering markets Implications for European digital sovereignty', available at https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf;jsessionid=1B1EAD40D8EDDC95B478C361DEAA45E6?__blob=publicationFile&v=1

[18]'OTT regulation should keep consumer interest in consideration: CUTS International', available at https://cuts-ccier.org/ott-regulation-should-keep-consumer-interest-in-consideration-cuts-international/. Please also see 'IAMAI slams COAI over revenue sharing demand that may dilute net neutrality', available at https://www.business-standard.com/article/economy-policy/iamai-slams-coai-over-revenue-sharing-demand-that-may-dilute-net-neutrality-123022300696_1.html and 'IAMAI opposes revenue sharing between OTTs and telcos', available at https://economictimes.indiatimes.com/industry/telecom/telecom-news/revenue-share-underhanded-attempt-to-violate-net-neutrality-iamai-on-coais-demand-of-compensation-by-otts/articleshow/98169929.cms?from=mdr

S. No.	Nature of Challenges	Observations and Recommendations
1.	Selective banning may be counter-productive	At the outset, selective banning of OTT services would primarily impact consumers who depend on such services to, for example, remotely work, attend classes, or conduct business. Since users may no longer be able to access their preferred OTT service and use the same for legitimate reasons, we believe that selective banning should not be pursued as a policy tool. Switching to alternatives – In addition to the above, lessons may be learnt from previous efforts undertaken in countries that have resorted to selective banning. For instance, users shifted to Signal as a result of the US Government announcing a ban on WeChat.[19] Therefore, the possibility that users will automatically shift to smaller and open source-based means of communication in the event their preferred OTT platform is blocked always exists. Accordingly, selective banning is not a one-stop solution to deterring the spread of misinformation or illegal activities online – an aspect which we understand to be the primary reason behind exploring the feasibility of selective banning. In addition, if users switch to less popular OTT services, LEAs may find it difficult to reach out to these platforms and obtain assistance from them, as their service providers may not have a Resident Grievance Officer, Chief Compliance Officer or even Nodal Contact Person – as required under the Intermediary Rules. Usage of VPNs – In addition, the technological advantages of VPN services may make the process of selective banning redundant. For context, there was a jump in usage of VPNs when Russia banned Facebook and Instagram a few years ago.[20] VPNs were also on high demand to access social media platforms in Jammu and Kashmir after a number of internet shutdowns.[21]
2.	Violation of the proportionality principle	Impinging upon fundamental rights As noted earlier, users rely on OTT services as part of their day to day lives, including to communicate with each other freely and even carry out small businesses via OTT platforms. Selective banning of OTT services may hamper users' fundamental rights under Article 19(1)(a) and Article 19(1)(g) of the Constitution. This is in light of the fact that the Supreme

[19]'China appears to block Signal, one of last popular encrypted messaging apps', available at https://www.livemint.com/technology/apps/china-appears-to-block-signal-one-of-last-popular-encrypted-messaging-apps-11615915217474.html.

[20]Russians' demand for VPNs skryrockets after Meta block, available at https://www.reuters.com/technology/russians-demand-vpns-skyrockets-after-meta-block-2022-03-14/.

[21]VPN apps in demand in Kashmir to make up for low-speed 2G, available at https://www.newindianexpress.com/nation/2020/feb/03/vpn-apps-in-demand-in-kashmir-to-make-up-for-low-speed-2g-2098369.html.

S. No.	Nature of Challenges	Observations and Recommendations
		Court of India in the landmark Anuradha Bhasin case (W.P. (C) No. 1031 of 2019) had noted that these fundamental rights can be exercised over the internet as well. Since selective banning will likely curb these fundamental rights, it is vital to ensure that the proportionality principle is satisfied before the Government adopts the same as a policy tool. As per this principle, the State can restrict fundamental rights to achieve a legitimate goal provided that the said restrictions are minimum, and the State has no better alternatives. At this stage, there is a lack of clarity on whether selective banning of OTT services is the best possible solution available to tackling unlawful content online or maintaining law and order during times of public unrest. Separately, we believe that blocking an OTT service is only a proportional response where such service has failed to comply with any applicable law or its obligations under such law, in which case Section 69A of the IT Act would anyways apply. Section 69A has been used by the Central Government to block entire OTT platforms on the ground of national security.[22]
3.	Concerns with URL-level blocking	The Department of Telecommunications, in the Parliamentary Standing Committee's Report on 'Suspension of Telecom Services/Internet and its Impact', had observed that: "services hosted on cloud are difficult to ban selectively since they operate from multiple locations in multiple countries and continuously shift from one service to the other. However, websites operating through fixed URLs can be banned." We agree with the fact that it is easier to selectively banning websites since they have fixed domain names and URLs, making their IP addresses easy to identify and block as well. However, it should be noted that users may attempt to circumvent such a ban, for example, by relying on VPN services available for use in India.
4.	Concerns with application-level blocking	In terms of selectively banning OTT services that are application-based, the following challenges arise: <u>OTT level blocking-</u> In this case, OTT service providers will have to obtain location information of their users to block their services in a specific geographic area. However, OTT service providers may not always have access to such information on account of a users' privacy settings, etc. They may also have to comply with

[22]Please see 'Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order', available at https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206; 'Government Blocks 118 Mobile Apps Which are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order', available at https://pib.gov.in/PressReleasePage.aspx?PRID=1650669

S. No.	Nature of Challenges	Observations and Recommendations
		requirements under the Rules for Data Privacy and Security Practices, as well as the upcoming DPDP Bill before accessing any such information. TSP-level blocking- TSPs can attempt to selectively block OTT applications by using the destination IP addresses of all the servers that an OTT service provider has used, but this task can be challenging. This is because, an OTT service provider may not want to share its IP addresses with a TSP and subsequently expose itself to potential cyber security incidents. Instances of over-blocking- Moreover, and as pointed out by the Department of Telecommunications, OTT services are typically hosted on the cloud and have their own dynamic IP addresses. If a TSP has to rely on such IP addresses for the purpose of pursuing selective blocking, it can lead to a situation where other OTT services that are hosted on the same cloud service and that use the same dynamic IP address are accidently blocked as well. While deep-packet inspection carried out by TSPs can prevent such a situation of over-blocking, the same, if pursued, will lead to far-reaching legal implications. This is because, TSPs (assuming they are able to access dynamic IP addresses in real time) would have to investigate each packet of data shared over the Internet in order to identify the specific OTT service that needs to be blocked. Since TSPs will have to intercept and investigate each packet of data being transmitted online, this raises free speech and net neutrality concerns.

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.

In light of our response to Question 10 above, we recommend against introducing any framework that will permit selective banning to take place. Thus, any additional framework for selective banning under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 or any other law, in force is not necessary at this stage. The existing legislative framework under the IT Act contains adequate provisions for pursuing blocking of online content, as well as entire OTT services. For example:

- Section 69A of the IT Act read with the Rules for Blocking allow for the blocking of online content (including an entire OTT platform) on certain grounds, such as sovereignty and integrity of India,

national security, public order, etc. Section 69A has been previously used by the Central Government to block numerous OTT platforms on the ground of national security. [23]

- In addition, blocking access to online content on certain grounds is also allowed under Section 79 of the IT Act read with the IT Rules.

In conclusion, the existing legal framework under the IT Act ensures that public's right to access an OTT service as well as an OTT service provider's ability to offer its services users does not face unwarranted interference, while simultaneously empowering the Government and regulatory authorities to take action against an OTT platform or against content hosted on such a platform, where required.

Q12. In case it is decided to put in place a regulatory framework for selective banning of OTT services in the country, -

(a) Which class(es) of OTT services should be covered under selective banning of OTT services? Please provide a detailed response with justification and illustrations.
(b) What should be the provisions and mechanism for such a regulatory framework? Kindly provide a detailed response with justification.

AND

Q13. Whether there is a need to selectively ban specific websites apart from OTT services to meet the purposes? If yes, which class(es) of websites should be included for this purpose? Kindly provide a detailed response with justification.

We recommend that there is no need to introduce regulations to selectively ban OTT services or websites (as explained in Question 11 above). Accordingly, we do not have any inputs to provide to these questions.

Q14. Are there any other relevant issues or suggestions related to regulatory mechanism for OTT communication services, and selective banning of OTT services? Please provide a detailed explanation and justification for any such concerns or suggestions.

Response: We do not have any further inputs to provide on the regulatory mechanism for OTT services, or on selective banning of OTT services.

***

[23] Please see 'Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order', available at https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206; 'Government Blocks 118 Mobile Apps Which are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order', available at https://pib.gov.in/PressReleasePage.aspx?PRID=1650669