From: Asaggarwal@nasscom.in
To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>
Cc: Varun@nasscom.in, Tejasvi@nasscom.in, Sudipto@nasscom.in
Sent: Friday, September 1, 2023 2:36:13 PM
Subject: Nasscom's feedback to the Consultation Paper on OTT Communication Services

Dear Shri Akhilesh Kumar Trivedi,

Kindly find attached Nasscom's feedback to the Consultation Paper on "Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services" released by TRAI in July 2023.

In case of any further information or query, please feel free to reach out to us.

Best regards,

Ashish

Ashish Aggarwal I Vice President, Public Policy I +91 120 4990196 I +91 9818008123 I Sector 126, NOIDA

nasscom

nasscom

Nasscom's Feedback on Telecom Regulatory Authority of India Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services

Shri Akhilesh Kumar Trivedi,
Advisor (Networks, Spectrum and Licensing)
Telecom Regulatory Authority of India
September 1, 2023

SUMMARY OF FEEDBACK

ISSUES RELATED TO REGULATORY MECHANISMS FOR OTT COMMUNICATION SERVICES

1. Disproportionate regulatory burden should not be imposed on OTTs as it can impede the virtuous cycle OTTs have contributed to in the data economy. Further, this can hamper consumer's right to choose, raise cost of service, create entry barriers and scuttle innovation in the OTT market. The government should explore options to **reduce some of the regulatory burden on the heavily regulated TSPs** under the licensing framework. This would promote ease of doing business and the data economy of the country.

2. A **market driven and organic collaborative framework** already exists in India between TSPs and OTTs. Any regulatory framework/intervention for revenue sharing model like network usage fee between TSPs and OTTs should be avoided as it could violate the principles of net-neutrality, distort competition and can negatively impact the diversity of products, prices, and performance.

3. Attempting to contain all OTT services, digital services, and apps in a single definition cannot account for **technological changes** & will be **too broad** for any regulatory purpose. Therefore, '**OTT services**' should not be defined.

4. OTT application can have multiple functionalities that are inextricably interlinked. Any attempt to delineate any of these features would be **artificial** and could lead to **market fragmentation**. Thus, there is no need for any classification of OTT services.

5. Certain obligations (as listed by TRAI in the consultation paper) vis-à-vis OTT providers are applicable only to telecom service providers (**TSPs**) because only **TSPs own exclusive rights to use public assets like – spectrum, numbering resources, right of way and critical infrastructure**. Whereas OTTs merely operate on the network layer of TSPs, and they are both technologically and functionally different from TSPs. Hence, the said comparison of obligations is not merited.

6. OTTs are regulated in the country under various laws – for example, Information Technology Act, 2000 (**IT Act**) and the Digital Personal Data Protection Act, 2023 (**DPDPA**), Competition Act, 2002and the Consumer Protection Act, 2019.

ISSUES RELATED TO SELECTIVE BANNING OF OTT SERVICES

7. Selective blocking of OTT services at the application-level (**by OTT service provider or TSPs**) does not appear to be practicable nor technically feasible.

8. The IT Act & Rules already contain comprehensive provisions to address security concerns, including blocking of information in emergency situations. The recently legislated **DPDPA** has provisions of blocking in the interests of public. There does not appear to be a case of additional regulatory framework for selective banning of OTT services under the current framework or any future law.

9. Selective banning of OTT services or platforms **even for a specific period** is likely to be **counterproductive** for consumers, small and medium scale business both in urban and rural sector who are dependent on these OTT services.

nasscom

INTRODUCTION

Nasscom welcomes the opportunity to submit our response to the Consultation Paper on "*Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*" (**Consultation Paper/Paper/CP**) released by TRAI in July 2023[i].

The premise of the CP, is the **back reference** from the Department of Telecommunications (**DOT**) in 2022 where DOT had requested TRAI to:

1. Reconsider the 'Recommendations on Regulatory Framework for Over-The-Top (OTT) Communications Services' of 2020 (**2020 Recommendations**); and
2. Suggest a suitable regulatory mechanism for OTTs, including the issues relating to 'selective banning of OTT services' based on the 26th report of the Parliament's Standing Committee on Communication and Information Technology on 'Suspension of Telecom Services/ Internet and its impact' of December 2021.

In the CP, TRAI has clarified that it responded to DOT's back reference in November 2022 where it was communicated to the DOT that issues associated with regulation of OTTs raised by DoT in its back reference to TRAI have **already been addressed with justifications in 2020 Recommendations**.[ii]

Given this background, it is not clear why this fresh consultation has been called for on **Point 1 above i.e., reconsideration of the 2020 Recommendations**. This is coupled with the fact that public consultation was already held on regulatory aspects of OTTs under the draft **Telecommunication Bill, 2022**.

It is pertinent to note that nothing has changed in terms of technical working of the OTTs since the last recommendations of TRAI, hence the need to relook at the regulatory mechanism requires some explanation by the TRAI but the same is absent in the consultation paper.

Notwithstanding the above, we provide our response to the Consultation Paper below.

OVERALL FEEDBACK

As we have submitted in our past representations that telecommunication services provided by TSPs include fixed and mobile telephone services (including internet connectivity), and data transmission services. TSPs provide these services through a license granted by the government which confers to them an exclusive right to acquire and exploit scarce natural resources like spectrum, numbering resources, and the right of way to set up infrastructure, among others. OTTs facilitate the exchange of information over the internet. Internationally, it is well recognised that the communication OTTs are different from traditional telecom services. The ITU has repeatedly emphasised this.[iii]

Further, OTT platforms provide **device synchronicity** i.e., they can be accessed through multiple internet-enabled devices simultaneously whereas TSPs cannot because of the hardware requirement of a SIM card. Given the rapid pace at which OTT platforms innovate and grow, these differences between OTTs and TSPs will only increase in the future.

Therefore, the fundamental differences between OTTs and TSPs continue to remain and hence, they are neither the same nor similar services which are substitutable in nature. These differentiations have been amply discussed in the previous years and have also been noted by TRAI in their previous consultation papers and recommendations over the past years.

While the TRAI in the CP has given a list of obligations imposed on TSPs vis-à-vis OTT providers (**see, page 44**), we believe that this is an incomplete picture. The obligations listed for TSPs (which are not applicable on OTTs) are the ones emanating from the fact that the TSP own assets (spectrum and numbering resources, etc.) and hence are liable to meet these obligations. As submitted in our past submissions that these obligations cannot be levied on OTT service providers as they run on top of the telecom networks.

Instead of increasing the telecom led regulatory burden on the communication OTTs, we submit that the government should explore options to reduce some of the regulatory burden on the heavily regulated TSPs under the licensing framework. This would promote ease of doing business and the data economy of the country. Further, we re-iterate that the OTTs are already sufficiently regulated in the country under various laws (**Please see response to Q no 5 and 7**).

Further, any disproportionate regulatory burden can impede the virtuous cycle OTTs have contributed to in the data economy. To illustrate, we draw inference from the growth of monthly wireless data usage, ARPU for data consumption and wireless internet subscriber base. For instance, the TSPs' revenue from data usage has increased more than **10 times from 8% to 85% in the last nine years i.e., from 2013 to 2022** (**See, Figure 1**). [iv]

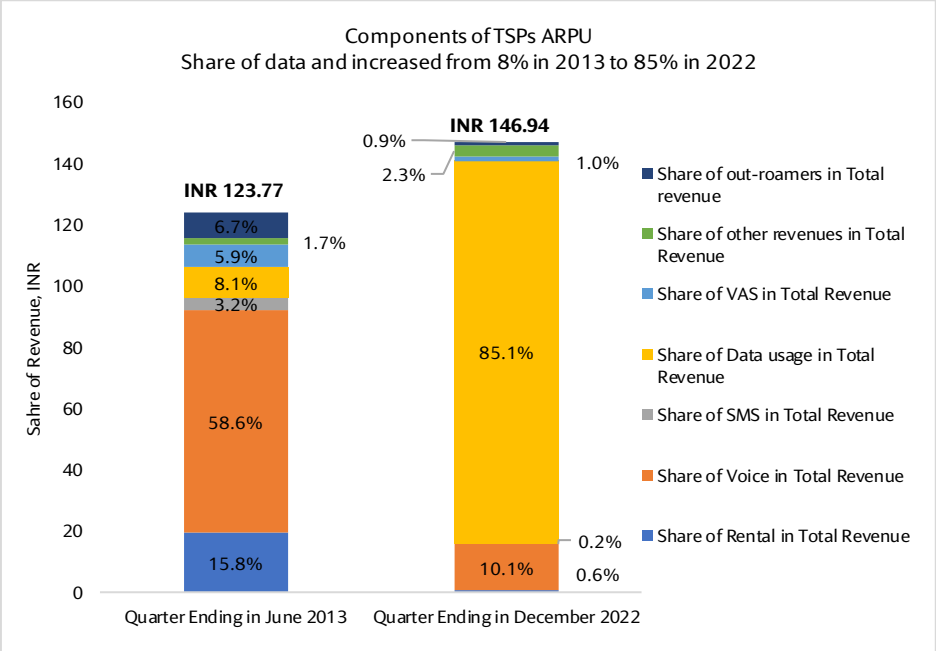
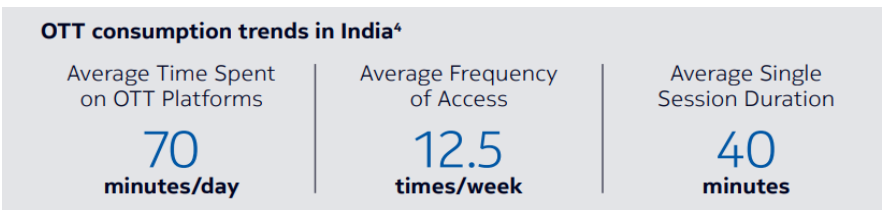


Figure 1

As per the Nokia Mobile Broadband Index 2020, on average, an Indian users spend approximately 70 minutes a day on OTT platforms, with each session lasting 40 minutes. [v] During and post covid, the data consumption has increased exponentially. TRAI in the CP has cited the ITU report of 2021 which states how internet became a necessity during the pandemic and OTTs were accessed by people for various critical activities.[vi]



Given this position, it is clear that OTT services have had an overall positive impact on the revenues of TSPs. Further, TSPs **partner with OTTs to offer bundled services that attract subscribers, build customer loyalty, and increase user spends on mobile and broadband services**.[vii] This was observed during a 2019 study conducted in India, Australia, Singapore, Thailand, & Philippines.[viii]

We believe that the licensing/ regulatory regime should be designed using an **activity-led and risk-based approach** that ensures obligations on an activity are **proportionate to the harms & risks** associated with it whilst keeping in mind the need to **avoid regulatory overlaps**. As stated, OTTs are sufficiently regulated in the country under various laws on several aspects, like privacy and security, lawful interception, etc (**discussed in response to Q no 5 and 7**). For instance, on safety aspects OTTs are proactively taking measures to identify and block suspicious accounts. This was recently acknowledged by the Union Minister, MeitY, Communications & Railways.[ix]

Hence, we believe that there is no need to introduce any additional regulatory regime as such a move may hamper consumer's right to choose, raise cost of service, create entry barriers and scuttle innovation.

Finally, we would like to state that blocking of internet/ services is a sensitive issue and due caution needs to be exercised while issuing any such order. As seen in the past, internet shutdowns or suspensions can have disproportionate negative effects. Today, given the increased adoption of digital payments and various other digital services, internet shutdowns have far greater negative consequences in disrupting the daily lives of the citizens, especially when internet shutdowns have been used for routine policing and administrative purposes which neither amount to public safety concerns nor public emergency[x]

Similarly, banning specific services like OTTs can have severe implications for civil liberties including free speech. In addition to this, there are significant economic costs. Estimates from the Internet Society suggest **losses caused by internet shutdowns crossed INR 187 billion in 2022**.[xi]

Thus, internet shutdowns or even selective banning of OTT services is not the best way to deal with situations of unrest. On the contrary, it may adversely affect users and local communities who are dependent on OTT services for legitimate use.

DETAILED FEEDBACK

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.

The CP rightly notes that "*...changes in network technology have supported the creation of an ecosystem of online applications including over-the-top (OTT) services...*" (emphasis added). The growth of the internet has led to the proliferation of digital services. While the terms "digital services" and "OTT services" are sometimes used interchangeably, it is important to note that they are comprised of a wide range of services (include online buying and selling, OTT communication and messaging services, OTT video streaming services, digital news, search services, navigation services, cab services, delivery, logistics services, etc.) with a wide range of functionalities.

The meaning and definition of '**OTT services**' has changed over time due to technological advancement and innovations in using those advancements. "OTT" is now used to mean practically all services provided via the public internet and includes the entire app ecosystem.

Rigidly defining concepts based on a current understanding essentially "freezes" the meaning to the time and context in which the definition is made. Such a definition does not and cannot account for changes in how technology and services are used. Attempting to contain all OTT services, digital services, and apps in a single definition will result in a classification that is simply too broad to be meaningful for any regulatory purpose.

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.

An OTT application can have multiple functionalities that are inextricably interlinked. For example, cab applications connect drivers and passengers, allow them to communicate, plan routes, enable payments, and more. The application requires all these features to work in tandem to provide a cab service. Similarly, food delivery services also have similar kind of features including communicating with the App provider, restaurants, payments, etc.

Any attempt to delineate any of the above features (say the communications service) from the cab service/ food delivery services would be artificial and could lead to market fragmentation. As a result, there is no need for any classification of OTT services.

It may be noted that there are already obligations under **IT Rules 2021** for significant social media intermediaries (**SSMI**) that provide services primarily in the nature of messaging are required to enable the identification of the first originator of information, in case of being served with a court order or the competent authority under the IT Act. [xii]

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.
&
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.

Please refer to our response to question no 1 and 2.

As stated above, communication is an integral part of most of the OTT services, be it cab services, food delivery apps, online grocery stores (big basket, milk basket, etc.). **It is thus difficult to sub-categorise the OTT communication services, and OTT services should be treated in its entirety**. In terms of regulations, there already exist various provisions under different Acts/ rules to sufficiently regulate them (**Please see response to Q no. 5**).

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.

As discussed above in the section on **Overall Feedback**, certain obligations are imposed on TSPs because they exclusively own spectrum and numbering resources and hence, such obligations cannot be extended to OTTs. In other words, comparing such obligations between TSPs and OTTs would be inaccurate (**See page 44 of the CP**).

A correct depiction would have been to show the kind of activities both TSPs and OTTs undertake along with the corresponding obligations. Please refer our submission to draft Indian Telecommunications Bill, wherein we had given an indicative table. [xiii]

Having stated this, for the services provided by the OTTs, and the aspects listed in question no 5 above, relevant obligations already exist and some of these are listed below:

Sl. No.	Aspect under consideration	Relevant Obligations
(a), (c), (d), (e),	**Regulatory aspects – privacy, security, safety**	As discussed in our introduction, that OTTs including communication OTTs are well regulated in India. We list here below the regulatory framework which governs privacy, security, and safety aspects of OTT communications services under the IT Act & Rules issued thereunder. These are: i. All body corporates (which includes 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**).[xiv] 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. ii. 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 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.[xv] iii. **Section 69A** 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.[xvi] iv. **Section 69B** read with **Rules for Monitoring Traffic** 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. v. **Section 79** read with **Intermediary Rules** prescribes the intermediary liability framework (OTTs are intermediaries) where intermediaries must act as a passive agent (or distributors) insofar as the illegal content is concerned, must observe "due diligence" conditions, and disable access to unlawful content upon receiving "actual knowledge" thereof.[xvii]

		vi. The **CERT-In framework**, along with the **SPDI Rules** contain many obligations to handle cyber-security incidents and to maintain privacy.[xviii] vii. In addition to the above, OTTs are covered as **data fiduciaries** under the recently legislated **DPDPA**. As per this law, OTTs are required to adopt/implement security practices/measures to comply with the obligations under the DPDPA. Further, OTTs are likely to continue to be regulated as **intermediaries** under the proposed Digital India Act which would replace the IT Act.
(b)	**Economic**	There is no need for economic regulation of OTT communication. The market for OTT communication is highly competitive and more than one service can be used at any given time, unlike network service providers/TSPs. Additionally, OTT services do not make use of scarce natural resources (spectrum) but run on top of existing TSP networks. As already stated above in the **first section**, the OTTs are significantly contributing to the revenues of the TSPs, thus contributing to the GDP.
(f)	**Quality of service (QoS)**	OTTs are delivered over the public internet and hence their QoS depends on the underlying network infrastructure. The application layer upon which OTTs operate does not control the underlying network infrastructure – which is already regulated by TRAI. The performance and reliability of the network, including factors such as bandwidth, latency, and packet loss, directly impact the QoS experienced by users accessing OTTs and platforms. This has been reiterated in the CCI study which suggests that QoS offered by TSPs very strongly influences consumer choice.[xix] OTT services have a natural design to maintain a high QoS for their customers on account of competition in the OTT services market. Customers can very easily switch from one OTT service to another, given that various options are available to users to choose from. This has ensured that OTT service providers maintain a high QoS. For instance, OTT service providers take periodic feedback from the customer about the quality of voice calls, platform etc. to improve their services.
(g)	**Consumer grievance redressal aspects**	OTT services are already subject to grievance redressal requirements under existing frameworks, such as the consumer protection framework under the **Consumer Protection Act, 2019** and Intermediary Rules. Consumers can also report grievances while using social media platforms under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021).

In sum, there are sufficient regulatory mechanism in place for OTTs. Existing regulatory conditions have enabled the market to grow organically and provide consumers with choice of application. Low switching costs and high availability of alternatives give consumers agency to download and use multiple OTT communication services and to migrate between them easily.

Any additional regulatory intervention (like a licensing framework) will negate these advantages by imposing entry costs, increase the cost of service which could be passed on to consumers, and thereby stymy the virtuous economy OTTs are contributing to. The TSP market is an example of how burdensome regulation could result in limited consumer choice, with only two or three alternative service providers and high switching costs.

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.

At the outset, it is correct to state that competition already exists in the OTT market and consumers have enough choice and freedom to choose the services as per their requirements. Any regulatory intervention will undermine the competitive forces in the market and lead to market fragmentation. The premise of OTT services is that they operate in a market with low barriers to entry and it is innovation that helps these services to distinguish themselves from other competitors and generate value with respect to their services. There is no need to bring OTT services under licensing framework.

We also request you to refer our response to Q No 5 (a) and (b).

If the conversation is about promoting competitive landscape with the TSPs, then this question does not arise as we have already explained above that the TSPs and OTTs are significantly different. The complement each other and do not compete.

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.

We would like to reiterate that there is no need for any additional licensing/regulatory framework for OTT services. We have already explained that OTTs are sufficiently regulated for aspects covered by their services. **Please refer our response to Q no 5 and 6**.

However, we would like to list down the laws as applicable for various aspects raised by TRAI in the above question:

Sl. No	Aspect under consideration	Relevant obligations for TSPs	Relevant obligations for OTTs
(a)	Lawful interception	Yes Section 5(2) of Telegraph Act- Allows lawful interception. Section 69 of IT Act – Power of the Government to intercept, monitor or decrypt any computer resource. Section 69B of IT Act- Government can monitor and collect traffic data or information through any computer resource for cyber security.	Yes Section 69, Section 69A and Section 69B deal with different powers of the State to: • intercept, monitor and decrypt information generated, transmitted, received or stored in a computer resource (**Section 69**); • block public access to information generated, transmitted, received, stored, or hosted in any computer resource (**Section 69A**); and • monitor and collect traffic data or information generated, transmitted, received, or stored in a computer resource (**Section 69B**).
(b)	Privacy and security	Yes General Conditions, **Clause 37** - Unified License Agreement: Protecting confidentiality of information.	Yes i. body corporates (which includes 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**).[xx] 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. ii. 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 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.[xxi] iii. **Section 69A** 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.[xxii] iv. **Section 69B** read with **Rules for Monitoring Traffic** 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. v. **Section 79** read with **Intermediary Rules** prescribes the intermediary liability framework (OTTs are intermediaries) where intermediaries must act as a passive agent (or distributors) insofar as the illegal content is concerned, must observe "due diligence" conditions, and disable access to unlawful content upon receiving "actual knowledge" thereof.[xxiii] vi. The **CERT-In framework**, along with the **SPDI Rules** contain many obligations to handle cyber-security incidents and to maintain privacy.[xxiv] vii. In addition to the above, OTTs are covered as **data fiduciaries** under the recently legislated Digital Personal Data Protection Act, 2023 (**DPDPA**). As per this law, OTTs are required to adopt/implement security practices/measures to comply with the obligations under the DPDPA. Further, OTTs are likely to continue to be regulated as **intermediaries** under the

			proposed Digital India Act which would replace the IT Act, 2000.
(d)	Unsolicited commercial communication	Yes As per TRAI regulations issued from time to time.	Yes, voluntary steps. OTT services - that enable commercial communication on their platforms - have themselves implemented features that allow users to report or block the senders of unsolicited commercial messages and calls. Few OTT services offer users the ability to opt out or unsubscribe from marketing messages, instead of blocking the number entirely. Other features include **silence unknow callers** to filter out spam calls.[xxv]
(e)	Customer verification	Yes General conditions, **Clause 39.17 -** Unified License Agreement.	Yes Most of the OTT services conduct a customer verification before enrolling them. This is done through a one-time password (OTP), either on their phone numbers or email IDs. Also as stated in response to Q2 above, provision to identify the originator of information already exists under IT Rules 2021.
(f)	Quality of service	Yes **Clause 29** - Unified License Agreement General conditions.	Yes, voluntary steps. OTTs are delivered over the public internet and hence their QoS depends on the underlying network infrastructure. The application layer upon which OTTs operate does not control the underlying network infrastructure – which is already regulated by TRAI. OTT services have a natural design to maintain a high QoS for their customers on account of competition in the OTT services market. Customers can very easily switch from one OTT service to

			another, given that various options are available to users to choose from. This has ensured that OTT service providers maintain a high QoS. Also, see above response to Q No 5(f).
(g)	Consumer grievance redressal	Yes, Telecom Consumer Complaint Redressal Regulations, 2012 issued by TRAI.	Yes a. OTT services are already subject to grievance redressal requirements under existing frameworks, such as the consumer protection framework under the Consumer Protection Act, 2019 and Intermediary Rules. b. Consumers can also report grievances while using social media platforms under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021).

Some of the aspects listed by TRAI are not applicable on OTTs as they do not own assets and also do not connect to the PSTN. These are listed below:

(c) Emergency services

These can only be made applicable to the TSPs to enable toll free services is to ensure that subscribers are not charged for making calls during an emergency. **The OTT services run on internet and do not have any network of their own or connect to the PSTN, through which they would be able to provide these emergency calling services**. In case the internet is not available, the customer still can make these calls on the TSP network but will not be able to do so on OTT.

(h) & (i) Eligibility conditions and financial conditions

This is not applicable, since we believe that there is no need to introduce any new licensing or regulatory framework for OTT service providers. The aim of the Government should be to encourage more and more start-ups to create OTT products/ services instead of creating entry barriers in this space. OTTs compete based on their services and quality and consumers can easily use multiple application (multi-home) at the same time, so the need to have eligibility and financial conditions is not clear.

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.

Probably the above question stems from the ITU's recommendations (also stated by the TRAI in the CP) on introducing a collaborative framework between OTT services and TSPs that seeks to promote competition, consumer protection, consumer benefits, innovation, investment, infrastructure development, etc. [xxvi]

First, it is worth nothing that **framework referred by the ITU is a 'market driven' framework and not a regulatory framework**. Second, such a collaborative framework already exists in India. TSPs and OTTs collaborate to offer plans to the customers for their benefit. For example, a 2019 study conducted by Ovum (in the markets of India, Australia, Singapore, Thailand, and Philippines) found that **bundling can increase customer loyalty and spending on mobile and broadband data services**. The study found that 44% of respondents had spent more on their carrier plan because they were subscribed to an OTT media bundle.[xxvii]

Both are making significant investment in infrastructure development. While the TSPs make investments in setting up the telecom network infrastructure, OTTs make substantial investments in complementary network infrastructure such as content delivery networks (**CDNs**), undersea cables, data centres and more. These investments help optimise the delivery of content through telecom networks, enabling cost savings and enhanced quality of service for TSPs and users. CDNs enable faster page loads, reduced latency, and lower bandwidth cost. For instance, **Netflix's Open Connect program** and **optimised codecs** together have yielded substantial cost savings for ISPs, surpassing USD 1 billion worldwide in 2021.[xxviii]

A report by Analysys Mason on '**The Impact of Tech Companies' Network Investment on The Economics of Broadband ISPs**' notes that to deliver their content and applications to end-users more efficiently, OTT service providers invest significant amounts in hosting, transport, and delivery networks. OTT service providers have continued to increase their investment, and it is estimated that on average, between 2018 and 2021, the investment was approximately $120 billion annually. [xxix] These investments are only increasing with increase in consumption by the consumers. For example, in 2022, **Meta announced a collaboration with Airtel and Saudi Telecom** to expand its subsea cable called 2Africa Pearls which connects Africa, Europe, and Asia to India.[xxx]

In sum, it is evident that the present regulatory regime promotes collaboration between OTT service providers and TSPs driven by their business interests. This enables them to benefit from one another, as TSPs provide the network infrastructure for OTTs and OTTs offer content that boosts user demand, thereby increasing revenues for TSPs. This shows a relationship of mutual interdependence. In such a scenario, imposing any additional regulations on OTT services to promote collaborative framework is neither required nor viable.

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.

As stated above, the present regulatory regime already promotes collaboration between OTT service providers and TSPs. Also, in our introduction, we have already stated how OTT services have contributed significantly to the revenues of the TSPs and are serving the consumers as well as the country.

We are not clear why the issue of **net-neutrality** has been flagged in the question on collaboration. In the CP, the ITU has clearly defined collaboration (**as stated in our response to Q no. 8**) and it does not mention any revenue sharing model or network usage fee.

Perhaps if the question stems from concern of stakeholders (like, TSPs) who might have raised the issue of network usage fee, then we would like to clarify that why any such proposal would be in violation of the principles of net-neutrality. To substantiate, in case of a revenue model, net neutrality may be violated:

a. if different rates are charged to different OTT services, wherein large or more prevalent OTT services are required to pay a higher share of fees or revenue to TSPs.
b. TSPs with their own OTT services may automatically become exempt from any revenue sharing or network usage fees requirement.

A revenue share model may result in a situation where TSPs earn revenues from both the end-user who are paying for data access, as well as OTT service providers who reimburse TSPs for using their networks to transmit content.

It is erroneous to state that OTT service providers free ride on TSPs, since OTTs contribute immensely to the revenues generated by TSPs. On the contrary, it is the OTTs who are driving the revenues of the TSPs. In the absence of OTT services, the revenues of TSPs would be reduced drastically. Attempt like network usage fee will adversely impact both consumer choice and consumer access as the increased price could be passed on to consumers and access to certain OTT platforms may also be restricted or limited.

In this regard, it is also important to note the **example of South Korea**. The imposition of a network usage fee in South Korea also had notable impacts on the future of data and internet use in the country, with both foreign and domestic OTTs choosing to suspend or degrade their services, or simply exit the market rather than pay high interconnection charges to the ISPs. [xxxi] The regime has been criticised on various grounds because of the fact it has led to poor quality of content and network services, expected increased prices for end-users, decline in diversity of online content, and imposed entry-barriers in the OTT sector. [xxxii]

TRAI has cited the BEREC assessment of underlying assumptions of payments from larges CAPs (Content Application Providers) to ISP, October 2022 stating that given the current state of market, the mechanism of payment is not justified as **CAPs are contributing significantly to ISP revenues and that there is no evidence of a free ride**.[xxxiii]

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.
&
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.

It has been quoted in the Parliamentary Standing Committee report that DoT has already recognised the challenges of selective blocking.[xxxiv] **Based on the feedback from our members, we believe that there are technical challenges in selectively banning of OTT services**.

Selective blocking is possible in case of URL level blocking. This is because they have fixed domain names. The government has been issuing orders for selectively blocking of websites by specifying URLs. However, this could be bypassed using Virtual Private Networks (**VPNs**) to camouflage IP addresses.

In case of **Application-level blocking**, this is envisaged in two ways:

a. **By the OTT service provider**: It is not possible to block services by a particular OTT service provider as this must be done for a specific geographic area, for which they will either need the **cell identification** from the TSPs or location details of all the users. Both these will not be made available by TSPs to the OTT Service providers due to privacy concerns under the new data protection law. Further, OTTs players cannot effectively block users using their IP addresses because as discussed above, it will not serve the purpose if someone is using VPNs.

b. **By the TSPs**: The TSPs may be able to selectively block fixed URLs or using the destination IP. However, sharing of IP addresses by OTT services/websites poses the risk of hacking and denial of service attacks on their infrastructure, making OTT services/websites resistant to sharing this information. Further, as noted by DoT in the Parliamentary Committee report, destination IP addresses of servers used by OTT services providers are often either **masked or hosted on the cloud and tend to be dynamic**.

   If TSPs map IP addresses in real-time, they will be required to inspect each piece of data passing through it to identify those which are to be blocked. This would involve immense investments by TSPs and will impact user experience through increased costs.

Therefore, selective blocking of OTT services at the application-level does not appear to be practicable or feasible.

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.
&
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.

As has been stated by TRAI in the CP, provisions exist in both the Unified License (**Clause 2.1, Chapter IX, UL (Internet Service)**) [xxxv] and IT Act (**Section 69A**) [xxxvi] for blocking of content. TRAI has also stated the detailed procedure is defined under the Procedure and Safeguards for blocking of Access of Information by Public. [xxxvii]

As is seen above, the IT Act & Rules already contain comprehensive provisions to address security concerns, including blocking of information in emergency situations. These provisions have also been used to block not only particular content or information, but entire websites and applications by the government. The recently introduced DPDPA also has provisions of blocking in the interests of general public. [xxxviii]

Therefore, there is no need for an additional regulatory framework for selective banning of OTT services neither under the current framework nor any future law. The present Acts and Rules have sufficient provisions to block online content. Any attempt to introduce any fresh regulations/ guidelines will only overlap with the existing Rules and may create ambiguity.

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.

While the **Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017** (**Telecom Suspension Rules**) prescribe detailed procedure to issue orders of internet shutdown, the same is not being followed by State governments in letter and spirit. The same has also been noted by the Parliament's Standing Committee on Communication and Information Technology in its 26th report titled 'Suspension of telecom services/ Internet and its impact.' [xxxix] The report states that suspension Rules have been grossly misused by ordering suspension on flimsy grounds leading to economic and other losses to the country. [xl]

The Supreme Court of India has also recognised that the right to freedom of speech and to carry on trade and business using the medium of the internet is constitutionally protected under Article 19 of the Indian Constitution. [xli]

It is also important to note that the impact of these internet shutdowns has not been assessed by the Government. A report by ICRIER, '**Anatomy of an Internet Blackout**', [xlii] which analysed the internet shutdowns in the country in detail has given examples of how some of these internet shutdowns have had a counterproductive effect.[xliii]

We believe that selective banning of OTT services or platforms may be counterproductive as most of the consumers are dependent on many such services for various purposes, including studying, working, watching content, etc. Many small and medium scale business both in urban and rural sector are dependent on these OTT services. Banning these services even for short durations would hamper the lives of consumers and their businesses. This has also been substantiated by **ICRIER in their report**.[xliv]

There is a need to look at the overall perspective of blocking/ banning of internet or OTT services.

For any queries related to this submission, please contact:

Ashish Aggarwal (asaggarwal@nasscom.in), or Vertika Misra (vertika@nasscom.in) or Sudipto Banerjee (sudipto@nasscom.in) with a copy to policy@nasscom.in.

About nasscom

Nasscom is the premier trade body and chamber of commerce of the Tech industry in India and comprises over 3000 member companies including both Indian and multinational organisations that have a presence in India. Established in 1988, nasscom helps the technology products and services industry in India to be trustworthy and innovative across the globe. Our membership spans across the entire spectrum of the industry from start-ups to multinationals and from products to services, Global Service Centres to Engineering firms. Guided by India's vision to become a leading digital economy globally, nasscom focuses on accelerating the pace of transformation of the industry to emerge as the preferred enablers for global digital transformation. For more details, kindly visit www.nasscom.in.

End Notes:

[i] See, Telecom Regulatory Authority of India, 'Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services' (July 2023).
[ii] See, para 1.8 at page 4 & para 1.9 at page 6 of the TRAI CP.
[iii] See, para 2.45 at page 27 of the TRAI CP.
[iv] See, Table 21 at page 12 of the TRAI CP.
[v] See, Nokia Mobile Broadband Index 2020 (page 8).
[vi] See, Para 2.22, page 19 of the TRAI CP: *ITU-D in its report of 202130 mentions that the COVID-19 "pandemic has highlighted that for most people the Internet is no longer just a convenience, but a necessity. People with reliable Internet access have been able to use OTTs to more easily access and share critical health information, maintain contact with friends and family, work remotely, and otherwise mitigate the adverse impact of social distancing, quarantines and similar measures."*
[vii] All TSPs have increasingly started offering bundled plans as can be seen from their advertisements:

- BSNL offers free amazon prime video subscription to postpaid broadband users.
- ALTBalaji partners with Reliance Jio.
- Airtel and Hotstar announce strategic partnerships.
- VI partners Hungama to launch pay-peer view service.

[viii] See, Ovum, OTT Media Services Consumer Survey & OTT-CSP Partnership Study (2019).
[ix] See, Business Today, Centre discontinues bulk SIM connections to curb cyber frauds, blacklists 67,000 SIM dealers, August 17, 2023.
[x] See, Parliament Standing Committee on Information and Technology in its 26th Report on 'Suspension of Telecom Services/Internet and its impact'.
[xi] See, BQ Prime, The Economic Cost of Small Internet Shutdowns
[xii] See, Clause 4 (2) of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[xiii] See, Nasscom feedback on draft Indian Telecommunications Bill 2022.
[xiv] See, 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."
Also see, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Rules on Data Privacy and Security Practices**)
[xv] See, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (**Rules for Interception**).
[xvi] See, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (**Rules for Blocking**).
[xvii] See, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021) (**Intermediary Rules**).
[xviii]See, Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (**Cyber-security Rules**).
Cyber-security Directions of April 2022 issued under Section 70B(6) of the IT Act (**Cyber-security Directions** by CERT-In). 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 cybersecurity 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.
[xix] See, Competition Commission of India, Market Study on the Telecom Sector in India, December 2021.
[xx] 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."
Also see, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Rules on Data Privacy and Security Practices**)
[xxi] See, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (**Rules for Interception**).
[xxii] See, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (**Rules for Blocking**).
[xxiii] See, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021) (**Intermediary Rules**).

[xxiv]See, Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (**Cyber-security Rules**).
Cyber-security Directions of April 2022 issued under Section 70B(6) of the IT Act (**Cyber-security Directions** by CERT-In). 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 cybersecurity 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.

[xxv] WhatsApp, How to silence unknown callers.

[xxvi] See, para 2.73 at page 44 of the TRAI CP.

[xxvii] Ovum, OTT Media Services Consumer Survey & OTT-CSP Partnership Study (2019).

[xxviii] See, Netflix's Open Connect program and codec optimisation helped ISPs save over USD1 billion globally in 2021 (July, 2022).

[xxix] See Analysys Mason report on The Impact of Tech Companies' Network Investment on the Economics of Broadband ISPs, October 2022.

[xxx] See, Outlook India, Meta To Jointly Invest With Airtel In Telecom Infrastructure (2022).

[xxxi] See WIK-Consult report on Competitive conditions on transit and peering markets

[xxxii] See Internet Society's, 'Internet Impact Brief – South Korea's Interconnection Rules'

[xxxiii] See TRAI CP, paras 2.77 & 2.78 at pages 53, 54 & 55.

[xxxiv] See, TRAI CP, para 3.7, page 62-63.

[xxxv] See, TRAI CP, para 3. 9 at page 64.

[xxxvi] See, TRAI CP, para 3. 10 at page 64-65.

[xxxvii] See, TRAI CP, para 3. 12-3.13 at page 65-66.

[xxxviii] See, Clause 37(1) (b) of Digital Personal Data Protection Act 2023.

[xxxix] See, Parliament's Standing Committee on Communication and Information Technology in its 26th report titled 'Suspension of telecom services/ Internet and its impact

[xl] See, page 46 of the Report: *Suspension Rules have been grossly misused leading to huge economic loss and also causing untold suffering to the public, as well as severe reputational damage to the country. The Committee are of the view that when the Government's thrust is on digitization and knowledge economy with free and open access to internet at its core, frequent suspension of internet on flimsy grounds is uncalled for and must be avoided. There is a need to monitor the exercise of this provision so that these are not misused to the disadvantage of people at large.*

[xli] See, Anuradha Bhasin v UoI, Writ Petition (Civil) no. 1031 of 2019

[xlii] See, Report by ICRIER, 'Anatomy of an Internet Blackout'

[xliii] See, Report by ICRIER, 'Anatomy of an Internet Blackout', page 31 – *'In Jammu and Kashmir, some shutdowns were reported to have a counterproductive effect. People found alternate ways to access the Internet, navigating through systemic loopholes and circumventing the law. In Gujarat as well, the Patidar agitation continued to pick momentum, despite the mobile Internet shutdown as it also did in the preemptive shutdown in Haryana. There are several instances of Internet shutdowns not having been able to prevent mass mobilisation and civil unrest.'*

[xliv] See, Report by ICRIER, 'Anatomy of an Internet Blackout', page 59 – *'Many young people, who are taking to social media as a creative outlet, are affected by shutdowns. Students are also adversely affected as universities put their material online but networks are shut frequently. Additionally, young students are also digital entrepreneurs and run businesses online, for example, an Instagram photographer from Kashmir faced significant losses in business during the Internet ban.'*