From: "bharat bhatia" <bharat.bhatia@itu-apt.org>
To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>
Cc: "V Raghunandan" <secretary@trai.gov.in>
Sent: Wednesday, August 30, 2023 7:04:04 PM
Subject: IAFI Response to Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services

Dear Akhilesh Ji,

Enclosed please find IAFI response to Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services.

Kindly acknowledge receipt of this email and the attached file.

Warm Regards,

Bharat B Bhatia,
President, ITU-APT Foundation of India (IAFI)
Vice Chairman, Asia Pacific, World Wireless Research Forum(WWRF)
M: +91 981 017 3737

ITU APT Foundation of India (IAFI)

comments on TRAI Consultation Paper regarding

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

CONTENTS

Chapter 1

Introduction ITU-APT Foundation of India (IAFI)

The ITU-APT Foundation of India (IAFI) is a registered non-profit and non-political foundation registered under the Cooperative Societies Act of India. IAFI has been recognized by the International Telecommunication Union (ITU) as an international/ regional Telecommunications organization and has been granted the sector Membership of the ITU Radio Communications Bureau (ITU-R), ITU Development Bureau (ITU-D) and ITU Telecommunication Standardization Bureau (ITU-T). IAFI is also an affiliate member of the APT. IAFI has been working for the last 21 years to encourage the involvement of professionals, corporate, public/private sector industries, R&D organizations, academic institutions, and other agencies in the activities of the ITU and APT.

For more details regarding IAFI, please visit https://www.itu-apt.org/

Chapter 2

Executive Summary of views of IAFI

Section 3 of the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 promogulated by the Telecom Regulatory Authority of India (TRAI) in 2016 prohibits distributors from offering or charging discriminatory tariffs for data services on the basis of content. TRAI released another set of recommendations on 28th November 2017 regarding net neutrality. Department of Telecommunications (DoT) on 31st July 2018 accepted the TRAI recommendations and issued guidelines on net neutrality.

As per the guidelines issued by DoT:

a. Internet service providers (ISPs) should not use any discriminatory tactics with respect to hosting of content.
b. ISPs shall not charge different rates from different applications, websites and other content providers over the Internet to host their content and to make it accessible to the general public.
c. The terms of various license agreements' governing provisions of Internet services shall be amended to include provisions of non-discriminatory treatment, applications, exclusions and exceptions.
d. The terms of license agreements shall also include necessary traffic management practices as formulated by DoT.
e. All specialized services as prescribed by the government, such as automatic driving, remote diagnosis, and all services running on IoT are excluded from the applicability of net neutrality. These services can be prioritised for faster internet lanes.
f. All content delivery networks shall not be included within scope of any restriction unless directed by the government.
g. All monitoring and enforcement functions shall rest with DoT.
h. The licensee is prohibited from entering into any agreement or arrangement having the effect of discriminatory treatment of content.
i. ISPs shall not engage in blocking, throttling or paid prioritization of any website or any content.

Net neutrality or network neutrality ensures that all data on the internet should be treated equally by ISPs and governments, regardless of content, user, platform, application, or device.

IAFI notes that the Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services (Consultation Paper) deals with the length and breadth of different aspects of OTT services. OTT services, as the name implies, operate over the top of the internet services provided by telecom service providers (TSPs). TSPs charge their subscribers the full amount needed by them to run their network and as such have no further claim vis-a-vis OTT services, who provide services using the internet.

In view of the above, IAFI's view is that the market forces may be allowed to respond to the situation without prescribing any regulatory intervention for OTT services, and only specific regulatory interventions may be made for achieving better consumer experience. Such regulatory intervention should ensure that all OTT platforms behave in a fair way online, noting that it links a large user base to a large number of businesses. IAFI is against any "selective" or otherwise banning of OTT services in any form.

India's existing Competition Act, 2002 governs traditional Indian markets with digital market competition being outside its purview, so far. Standing committee on Finance (Ministry of Corporate Affairs), vide its 53rd Report (Dec 2022) discussed various issues related to needs of ex-ante regulations to regulate the growing digital markets which are at a nascent stage. It highlighted the need of having India's Digital Competition Act which is being prepared by the Ministry of Corporate Affairs and the Ministry of IT.

It is observed that under traditional telecom services, interoperability was an essential component. Different platforms were asked to provide suitable interfaces for a proper interconnect with other platforms. Such a mandated provision helped growing of different technologies and platforms in most competitive way resulting in a healthy penetration and adoption of telecom technologies in India. However, a similar interoperability is not existing amongst various OTT platforms.

IAFI has also noted that the impact on consumers due to lack of interoperability was the main focus of the recently implemented Digital Market Act (DMA) by the European Union. The Act also manages various other issues including some highlighted by the Authority.

In view of the above, IAFI view is that the market forces may be allowed to respond to the situation without prescribing any regulatory intervention and no regulatory interventions are required in respect of issues related to the OTT services. IAFI is against any "**selective" or otherwise banning of OTT services** in any form. However, regulator should ensure that all these platforms behave in a fair way online, noting that it links a large user base to a large number of businesses.

Chapter 3

Response to TRAI Questions

Q-1: What should be the definition of over-the-top (OTT) services? Kindly provide a detailed response with justification.

ITU-T D.262 recommendation on the definition of OTT services is as follows:

OTT services means services provided over the public internet that do not require a dedicated network or user equipment, and that is directly accessible by end-users. It is also mentioned in the recommendation that the definition of 'OTT' is a matter of national sovereignty and may vary among Member States.

ITU's definition is in line with several other definitions identified in the Consultation Paper:

a. The Organization for Economic Co-operation and Development uses the phrase "over the Internet"[1] to describe OTT services.
b. The Office of Communications, United Kingdom describes OTT services as being offered "over the top of an existing data network connection".[2]
c. The Body of European Regulators for Electronic Communications (BEREC), and the Commonwealth Telecommunication Organization describe OTT services as being offered "over the Public Internet".[3]

The above-mentioned definitions accurately capture the technical aspects of OTT services, and how they differ from telecom services. To begin with, TSPs operate on the **network layer** of the internet (which drives the operation of the internet), and OTT service providers operate on the **application layer** (which rests above the network layer and cannot function without it). In a nutshell, the network layer facilitates the transfer of data, content, and applications that are offered by OTT service providers.

Thus, keeping in mind the definitions mentioned above, TRAI may consider adopting the following definition of OTT services:

- An OTT service is either a content-based or application-based service that travels over the top of the public internet or over an underlying network connection to reach the end user.

Q-2: 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.

At the outset, OTT services have become increasingly popular in recent years, as they offer a number of advantages over traditional telecommunications services. These advantages include:

- **Lower cost**: OTT services often have lower costs than traditional telecommunications services, as they do not require the same level of infrastructure investment.
- **Greater flexibility and portability**: OTT services are more flexible than traditional telecommunications services, as they can be accessed from anywhere with an internet connection.

[1] Organisation for Economic Co-operation and Development (OECD) Communications Outlook (2013), at page 4, available at https://www.potraz.gov.zw/wp-content/uploads/2016/01/Consultation_OTT.pdf.
[2] The Office of Communications, United Kingdom, Mobile Call Termination Market Review 2015-18, at page 5, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0025/74257/annex_15_glossary.pdf.
[3] Body of European Regulators for Electronic Communications, Report on OTT Services, 2016, at page 3, available at https://www.berec.europa.eu/sites/default/files/files/document_register_store/2016/2/BoR_%2816%29_35_Report_on_OTT_services.pdf; and Commonwealth Telecommunication Organization, Report on Over The Top Applications & Internet Value Chain, 2020, at page 14, available at https://cto.int/wp-content/uploads/2020/05/CTO-OTT-REPORT-2020.pdf.

- **Wider range of features**: OTT services often offer a wider range of features than traditional telecommunications services, such as video chat, file sharing, and online gaming.

While OTT services vary in terms of the services and products they offer, the features of these varied products and services overlap extensively. For instance, several OTT services have features which can be categorised as communication-based features, as well as non-communication-based features. To elaborate, OTT services such as cab aggregators or food delivery platforms also allow users to communicate with drivers, restaurants, or customer care executives in addition to their main functions. Since there are commonalities in the features of different OTT services, attempting to categorise them further is not practical. Therefore, we are of the view that it is not necessary to identify the different categories of OTT services at this stage. As such, we have responded to TRAI's questions keeping in mind OTT services as a whole.

Q-3: 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.

As stated in our response to Question 2 above, we do not believe that it is necessary to identity categories of OTT services. As a corollary, there is no requirement to define "OTT communication services" at this stage. This is because there is no clear test that (i) identifies and distinguishes between different OTT services with their overlapping features and functions, and (ii) distinguishes communication-based services from non-communication-based services.

Instead, we have taken the opportunity to delve into the differences between OTT services. and telecom services We would like to reiterate that the most prominent characteristic is that OTT services are accessed and provided over the underlying network operated by TSPs. This means that OTT services operate on a different layer of the internet (i.e., the application layer) from TSPs (which operate on the network layer). Moreover, technically speaking, TSPs not only control the underlying infrastructure required to provide network services, but also have access to spectrum, the ability to interconnect with the Public Switched Telephone Network (PSTN), are entitled to right of way and so on.

In addition to this, TRAI, in the Consultation Paper, has observed that some OTT services are a direct technical and functional substitute for services offered by TSPs. This is an inaccurate description of the characteristics of OTT services. To elaborate, there are several functional differences between TSPs and OTT services. For example, TSPs provide internet access to consumers, while OTT service providers rely on the same internet access to provide a range of different services to users (as highlighted above). Therefore, from a user perspective, these services are not the same and definitely not substitutable. Indeed, most users are likely to use both types of services simultaneously or only use traditional telecom services.

Operationally speaking as well, the services offered by TSPs are critical in order for OTT service providers to gain access to the internet and reach the end user. Similarly, users must also purchase internet access from TSPs to access online services offered by OTT providers. It

is also expected that there will be fair rules between different OTT communication platforms which will help all players benefiting from fairer behaviours when doing businesses.

Q-4: 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.

For the reasons stated in our responses above, we do not believe that it is necessary to further classify OTT services, or even OTT communication services, into sub-categories. In light of this, we have tailored our responses to the questions in this Consultation Paper to focus on the overarching category of OTT services.

Q-5. 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.

OTT services and licensed telecommunication services in India differ in various aspects, including regulatory, economic, security, privacy, safety, quality of service, and consumer grievance redressal. Our comments on the above aspects regarding OTT services vis-à-vis licensed telecommunication services in India are as follows.

(a) **Regulatory aspects**:

i. We note that TSPs, in the past, have argued that the lack of regulation for OTT services creates an uneven playing field and poses challenges in terms of competition and revenue generation. They have called for the creation of a 'level playing field', suggesting that OTT services should be subject to similar regulatory requirements. We disagree with this approach. As noted above in our response to Question 3, there are various functional, technical, and operational differences between OTT services and telecom services. It is on account of these differences that TSPs are subject to a rigorous regulatory regime. This is not to say that OTT services are not regulated adequately in India. In fact, OTT services are subject to a variety of regulations under the Information Technology Act, 2000 (IT Act) and its rules on reasonable security practices (Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)), interception, monitoring, and

decryption, content-blocking (Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (Interception Rules)), and cyber-security (Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules) and CERT-In Directions of April 2022[4] (CERT-In Directions)). OTT service providers will also be regulated under India's recently passed data privacy law (i.e., the Digital Personal Data Protection Act, 2023 (DPDP Act)), as well as the proposed Digital India Act (DIA).

ii. Thus, there is no need to govern OTT services under telecom laws as well. Over-regulation could stifle innovation and limit consumer choices, in addition to adversely impacting the ease of doing business in India.

(b) **Economic aspects:**

i. OTT services have had a significant impact on the economics of the telecommunications industry. OTT communication services have created new revenue opportunities for licensed TSPs due to a sharp rise in data consumption by end-consumers. This is complemented by the fact that India is the second largest telecom market in the world with a subscriber base of over 1.17 billion.
   - Notably, the TRAI in the Consultation Paper recognises the growth in revenues earned by TSPs on account of a manifold increase in consumption of data. The following statistics (as cited in the Consultation Paper) as well as a report by the Indian Council for Research on International Economic Relations on 'State of India's Digital Economy' lend credence to our position, from 2012 to 2022, the monthly average revenue per user (ARPU) for wireless services in India grew by about 44% from INR 98 to INR 141.14.
   - volume of monthly wireless data usage grew from 2014 to 2022 by about 156 times from 92.4 million GB to 14.4 trillion GB.
   - the average revenue from data usage per wireless subscriber per month increased about 5.6 times from 2014 to 2022.
   - internet subscriptions have more than tripled from 248 million in 2014 to 820 million in September 2022.

ii. We would also like to refer to BEREC's paper titled 'BEREC preliminary assessment of the underlying assumptions of payments from large CAPs [content and information providers] to ISPs'. BEREC, while examining whether there is a need to implement a direct compensation model, noted that there is a mutual dependence between OTT service providers and TSPs, and OTT service providers cannot be said to free-ride over the services offered by TSPs. Moreover, according to BEREC, demand from ISPs' customers for content drives demand for broadband access; and the availability of broadband access drives demand for content. Notably, BIF's findings, in its report on

[4]That is, the 'Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet', issued by the Indian Computer Emergency Response Team dated April 28, 2022.

the 'Economic Value of the App Economy in India' also supports the argument that OTT services have contributed to the revenues earned by TSPs.

(c) **Security aspects**:

i. The IT Act contains various requirements on security practices and cyber-security. We believe that this is sufficient for the time being.
ii. For example, the CERT-In Rules, and the CERT-In Directions contain requirements that aim to bolster cyber-security within the country. These requirements include mandatory reporting of certain cyber-security incidents within specific timelines, maintenance of logs of ICT systems in order to facilitate cyber-incident reporting and so on. In addition, Section 69B of the IT Act read with the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (Traffic Rules) empower Government agencies to monitor and collect traffic data / information for cyber security purposes.
iii. Further, Section 43A of the IT Act read with the SPDI Rules mandated entities, including OTT service providers, to implement reasonable security practices and standards (such as having an ISO 27001 certification, maintaining information security policies, etc.) in order to protect all personal information / sensitive personal data or information in their possession.
iv. Additionally, the DPDP Act (which will replace Section 43A and the SPDI Rules once it has been enforced) imposes more stringent obligations on OTT services with respect to implementation of reasonable security practices and procedures. The DPDP Act also empowers the Government to direct any intermediary to block public access to any information on a computer resource that enables a data fiduciary to offer goods and services in India, in the name of public interest and under certain circumstances.
v. There is also Section 69 of the IT Act read with the Interception Rules and Section 69A of the IT Act read with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules) that enable Government agencies to issue appropriate directions to, for example, monitor or even block unlawful content on a computer resource on specific grounds.

(d) **Privacy aspects**:

i. The SPDI Rules, in addition to mandating reasonable security practices, contain a host of privacy related obligations that entities, including OTT service providers, must adhere to. This includes requirements relating to publishing a privacy policy, taking due consent prior to processing sensitive personal data or information, providing all relevant details to individuals whose data is being processed, etc.

ii. Additionally, as mentioned above, the DPDP Act has more stringent privacy obligations applicable to OTT services with respect to their users personal data. For instance, any consent taken from a data principal must be free, specific, informed, unconditional, and unambiguous. Such consent will be limited to processing only that

personal data which is necessary for the specified purpose. Further, a request for consent must be accompanied by a notice informing the data principal of (among other thing) the personal data collected and the purpose for which it is being processed. With respect to the processing of children's data, the DPDP Act imposes additional obligations, such as requiring verifiable parental consent, and restricting the data fiduciary from tracking, monitoring behaviour of, or targeting advertisements directed at children, or undertaking any processing that is detrimental to the well-being of children. There are incremental obligations on entities that fall within the category of significant data fiduciaries, among other things.

(e) **Safety aspects**:

i. OTT services implement their own internal measures to bolster the safety of their users. OTT services also have community guidelines and content moderation policies to curb the dissemination of harmful content on their platforms. They also generally enable users to report or block other user accounts keeping in mind the contours of such community guidelines and content moderation policies.

ii. Separately, to maintain the privacy and security of their platforms and of their users, OTT service providers also often mandate two-step verification in order for users to gain sign up and access to their platforms. They also empower users to implement privacy controls, such as keeping their profile private, etc.

iii. Further, OTT services have implemented increasingly novel ways to boost security of their platforms and ensure user safety. They have done so by implementing 'forward' limits on messages, placing 'labels' on misleading posts, etc.

iv. Lastly, the proposed DIA – which, as per public reports, will focus on bolstering user safety online – is also likely to impose a host of obligations on OTT service providers.

(f) **Quality of service aspects**:

i. OTT services should have different quality of service (QoS) requirements than licensed telecommunication services, as these services do not require the same level of reliability as traditional voice and SMS services.

ii. That said, OTT service providers often have their own internal standards to maintain the quality of their services. This is because the OTT services industry is a highly competitive one, given the low barriers to entry. Since there is a large variety of OTT services that exist in India, drop in quality of one service can lead to users switching to another competing service. This possibility automatically ensures that OTT service providers take the issue of maintaining QoS seriously.

iii. We believe that such self-regulation is sufficient for the time being, and there is no need to impose any mandated QoS standards on OTT service providers. Doing so may, among other things, prevent OTT services from constantly innovating and testing new features for their users. It may also impact their ease of doing business.

(g) **Consumer grievance redressal aspects**:

i. Laws such as the Consumer Protection Act, 2019 and the IT Act read with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules) contain grievance redressal requirements. For example, under the consumer protection framework, these requirements extend to paid online services, and under the IT Rules, these requirements extend to intermediaries. Given that most OTT services will qualify as intermediary platforms, they are subject to requirements such as appointing a grievance officer, handling complaints with specified timelines, etc.
ii. In addition to this, the DPDP Act also requires data fiduciaries to establish a grievance redressal mechanism for data principals, which in this case would be the end-users of OTT services.

Q-6. 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.

To bring OTT services under any additional licensing/regulatory framework is a complex question and not easy to answer. OTT services, being contributors to GDP growth, should not be regulated under any framework designed for traditional telecom services, because they are new and innovative services that should be allowed to operate freely. Excess regulation would stifle innovation in the online services sector and would not be in the best interests of consumers.

To elaborate, bringing OTT services under a new regulatory framework will likely lead to the following issues:

i. **Increased costs**: Regulation would increase the costs of OTT services for consumers, as the OTT providers would likely have to pass on the costs of compliance with regulations (especially vis-à-vis licencing related requirements where licence fee, etc. are imposed) to consumers. This will negatively impact consumers who may not be able to afford paid services.

ii. **Multiple frameworks**: Regulation would be unnecessary and superfluous because there are adequate laws in India that govern OTT services. There are also recently passed laws such as the DPDP Act and the DIA that will regulate OTT services (as detailed in our responses above).

iii. **Stifling of innovation**: Regulation would stifle innovation by making it more difficult for OTT providers to launch new services and features – a key factor for OTT services to remain relevant in a highly competitive industry. This could also slow down the pace of innovation in the OTT industry. In fact, OTT service providers may reconsider existing investments in technology innovation as well (in order to save operational costs).

IAFI recommends that there is no need bring OTT communication services under any licensing/regulatory framework. However some limited regulatory interventions may be needed to ensure interoperability amongst OTT platforms : Interoperability means the ability to exchange information and mutually use the information which has been exchanged through interfaces or other solutions, so that all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function. To ensure transparent interoperability, there is a need to create a 'Gatekeeper'. The gatekeepers would be required to ensure, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features that are available or used in the provision of its own complementary and supporting services and hardware. Such access can equally be required by software applications related to the relevant services provided together with, or in support of, the core platform service in order to effectively develop and provide functionalities interoperable with those provided by gatekeepers. The aim of the obligations is to allow competing third parties to interconnect through interfaces or similar solutions to the respective features as effectively as the gatekeeper's own services or hardware. The lack of interoperability allows gatekeepers that provide number-independent interpersonal communications services to benefit from strong network effects, which contributes to the weakening of contestability. In this process, to ensure interoperability amongst various platforms, adoption of necessary protocols which were should be mandated in India.

Q-7. 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, there is no need to bring OTT services under any additional regulatory framework as they are already adequately regulated by existing laws (as detailed in our responses above and reiterated below).

(a) **Lawful interception:**

The IT Act contains sufficient provisions to enable Government authorities to intercept communications on a given OTT communication service. Section 69 read with the Interception Rules relates to the power of the State to intercept, monitor, and decrypt information generated, transmitted, received or stored in a computer resource. Similarly, Section 69B read with the Traffic Rules enables the State to monitor and collect traffic data or information generated, transmitted, received, or stored in a computer resource. Further Section 69A gives the State the power to block public access to information generated, transmitted, received, or stored in any computer resource. For more details, please refer to our response to Question 5(c) above.

(b) **Privacy and security:**

Existing laws and regulations like the CERT-In framework comprising the CERT-In Rules and the CERT-In Directions and the SPDI Rules contain obligations that deal with cybersecurity incidents and privacy of individuals' personal information. Please refer to our comments in Question 5(c) and 5(d) for details on privacy and security aspects.

(c) **Emergency services:**

TSPs are required to offer emergency services including toll-free services to numbers designed 'police', 'fire', and ambulance under extant telecom laws. It is critical for TSPs to provide such toll-free services to ensure that their subscribers do not face any hurdles or disadvantages while attempting to make emergency calls.

There is, as such, no requirement to subject OTT service providers to similar obligations given that they need the internet to offer their communication services to users, and a user may not always have access to the internet during times of emergency. Moreover, many OTT services (including those that offer communication functionalities) do not interconnect with the PSTN or have the requisite infrastructure or equipment to broadcast emergency announcements. Lastly, in order to provide emergency services in furtherance of operations on search and rescue, OTT service providers may not always have access to the location of their users (depending on the privacy settings available on their platforms). Thus, OTT service providers are not the best-suited to provide emergency services.

(d) **Unsolicited commercial communication:**

Many OTT service providers that facilitate commercial communication services on their platforms have implemented features to enable users to take action against unsolicited commercial communication. For example, users can report or block those sending such communication, or even unsubscribe from the same.

(e) **Customer verification:**

OTT service providers already verify the identity of their users who wish to sign up to their services by way of one-time passwords (OTPs). That is, they require users to provide some form of identification, such as an email, address or mobile/phone number for the purposes of signing up.

This is in addition to the user verification requirement under the IT Rules wherein significant social media intermediaries (under whose ambit many OTT services fall) have to provide an option to their users to voluntarily verify their accounts and provide such users with a demonstrable and visible mark of verification, which should be visible to all other users of the service. Further, certain OTT service providers have entered into voluntary agreements with regulatory authorities to collaborate in instances where users with disconnected phone numbers continue to use OTT services where they used such phone number to sign up. In such cases, the OTT service provider re-verifies such accounts / numbers.

(f) **Quality of service:**

Please refer to our comments in Question 5(f) for details on QoS aspects.

(g) **Consumer grievance redressal:**

Please refer to our comments in Question 5(g) details on consumer grievance redressal aspects.

(h) **Eligibility conditions:**

Since we believe that OTT services should not be subject to any additional licensing or regulatory framework, this aspect is not relevant.

(i) **Financial conditions:**

Since we believe that OTT services should not be subject to any additional licensing of regulatory framework, this aspect is not relevant.

Q-8. 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 ITU's recommendations on 'Collaborative framework for OTT services' relate to introducing a collaborative framework that promotes competition, consumer protection, consumer benefits, innovation, investment, and infrastructure development. We understand that these are important aspects to consider. However, the existing business and economic environment in India already promotes these aspects. Thus, there is no need to introduce a formal collaborative framework for OTT service providers and TSPs, due to the following reasons as given below.

OTT services and licensed TSPs are two different but complementary sides of the same coin. OTT services provide the content and services, while licensed TSPs provide the infrastructure. In this regard, and as observed by the ITU in its report on 'Economic impact of OTTs on national telecommunication/ICT markets', TSPs and OTT service providers have often entered collaborative initiatives with one another in order to improve network infrastructure. OTT service providers have also made investments in developing passive internet infrastructure

across the globe. Even in India, they have invested in passive infrastructure and connectivity projects to improve internet access services.[5]

It would be pertinent to also refer to the findings of Analysys Mason in its report on 'The Impact of Tech Companies' Network Investment on The Economics of Broadband ISPs'. As per this report, OTT service providers have, on their own, invested significantly (approx. USD 120 billion annual from 2018 to 2021) in hosting, transfer and delivery networks to deliver content and applications to end-users in a more efficient manner. This has also helped the telecom industry save costs (approx. USD 5 to 6.4 billion each year globally).

Q-9. 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 formal collaborative framework between OTT service providers and the licensed TSPs is not necessary for the reasons highlighted by us in or response to Question 8 above. That said, we take this opportunity to also highlight few potential challenges that will arise if any such framework is implemented.

It is likely that a network usage fees (NUF) system may become an integral part of any such collaborative framework. If the same is implemented, it may lead to a situation where TSPs earn revenues from their subscribers who purchase data, as well as OTT services who will have to reimburse such TSPs for utilising their network to reach users. If TSPs are allowed to gain an extra source of income, courtesy OTT service providers, they may likely direct the same towards their own profits and not towards developing their network infrastructure and improving the quality of their services.

Net neutrality ensures that all internet traffic is treated equally without discrimination or preferential treatment. However, a NUF model is likely to go against the principle of net neutrality, especially if TSPs levy different rates for different OTT communication services depending on the scale or size of their operations, etc. Net neutrality (in addition to competition law principles) may also be violated if one considers the possibility that TSPs that own OTT services may be exempt from paying any NUF.

If OTT services are required to pay a fee to TSPs or provide compensation in any other manner, OTT service providers may find themselves in a position where they have to rollback investments in network infrastructure or reconsider existing initiatives to improve the quality

[5] As per reports, we understand that an industry alliance was founded by Meta to create network architectures to improve telecommunication infrastructure, available at https://telecominfraproject.com/facebook-partnering-to-build-the-telecom-infra-project/. Meta has also partnered with Airtel to develop subsea cable infrastructure, and Google has also been involved in subsea cable projects to improve global connectivity, including in India, available at https://indianexpress.com/article/business/airtel-partners-with-meta-to-develop-undersea-cable-infra-for-high-speed-internet-8307705/

of their services. Poor quality connectivity will adversely impact consumers in the long run, and would be antithetical to the country's goal of become a 'Digital India'.

Notably, South Korea's attempt to introduce the NUF model did not produce favourable results.[6] Instead, it resulted in rising consumer costs, the quality and diversity of content going down, and a slower internet with declining investments in network infrastructure. This has prompted a lot of pushback against the NUF model in South Korea.[7]

Lastly, we also refer to concerns raised by CUTS International and the Internet and Mobile Association of India on recent demands made by the telecom industry for the introduction of a NUF model between TSPs and OTT service providers.[8] These concerns, among other things, include the fact that smaller OTT services may be adversely affected. Consumers may also face an increase in cost of services as they will not only have to pay TSPs for network access but also OTT service providers for their services (i.e., in the event OTT services that are currently offered free of cost become paid to offset the added burden of NUF). Similarly, the imposition of higher costs associated with internet usage may disincentivize growth of OTT services in India and reduce their overall revenues.

Issues Related to Selective Banning of OTT Services:

The selective banning of OTT services is a complicated issue. Some arguments state that it is necessary to ban certain OTT services in order to protect national security or public order. Other arguments state that banning OTT services is a violation of freedom of expression and that it stifles innovation. Selective banning of OTT services presents complex challenges, involving considerations of freedom of expression, net neutrality, consumer choice, innovation, and privacy. It is essential for regulators to approach such decisions with careful evaluation, transparency, and a commitment to preserving a healthy and vibrant digital ecosystem. A balanced and well-informed approach is necessary to address concerns while promoting the benefits of an open and inclusive internet environment.

There are a number of potential challenges associated with the selective banning of OTT services. These include:

i. It is difficult to determine which OTT services should be banned, and which OTT services pose a threat to national security or public law and order. As a result, there is a risk that OTT services that are not actually harmful could be banned.

---

[6] As per this model, TSPs can charge fees for data traffic they receive from one another. As part of this, they have resorted to recovering these charges from OTT services.

[7] 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

[8] '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/; '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

ii. Banning specific OTT services could raise net neutrality concerns if the decision is based on content discrimination.
iii. Banning OTT services can stifle innovation. OTT services are a source of innovation and banning them can prevent new and emerging technologies from developing.
iv. Banning OTT services can violate freedom of expression. OTT services are a way for people to express themselves and banning them can restrict freedom of expression.
v. OTT service providers that are selectively banned may suffer financial losses, damage to reputation, and disruptions to their user base.
vi. Enforcing selective bans on OTT services can be technologically complex. As the digital landscape evolves rapidly, new services and platforms may emerge, making it challenging to keep up with enforcement efforts.

Thus, selective banning of OTT services is a complicated issue, and there are a number of potential challenges associated with it. IAFI is against any selective banning of OTT services.

Q-10. 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.

In addition to the aforementioned concerns we have with selective banning, we note that selective banning of specific OTT services and /or websites in specific regions of a country for a specific period presents several technical challenges. These challenges arise due to the distributed nature of the internet, the use of encryption, and the complexities involved in implementing precise and targeted blocking.

Some of the technical challenges in selective banning of specific OTT services and websites in specific regions of the country for a specific period are:

i. **Privacy concerns:** In the event an OTT service provider is directly required to block its OTT service in a specific region, it will need access to the location information of all its users. However, an OTT service provider may not always have access to such information – for example, due to users' privacy settings on the OTT service.
ii. **Dynamic IP addresses**: In the event a TSP is required to block an OTT service or website, it will need to gain access to the IP addresses of the servers used by the concerned OTT service provider. However, not all OTT service providers may be willing to provide such information on account of cyber-security concerns. Moreover, OTT services and websites are often hosted on cloud platforms and on servers with dynamic IP addresses. This means that the IP address of the server can change frequently, making it difficult to block access to the service or website.
iii. **Over-blocking and Collateral Damage**: Selective banning – by way of relying on the IP addresses of an OTT service or website's servers - can also result in over-blocking, where legitimate websites or services hosted on the same cloud platform and using the same IP address may get unintentionally blocked, causing collateral damage. Therefore, ISPs, that gain access to an OTT service's dynamic IP access, will likely have to regularly monitor and audit their block-list, to reduce over-blocking. One way to prevent this is to conduct a deep packet inspection (DPI), but that comes with its own challenges as highlighted below.

iv. **Content delivery networks (CDNs)**: Many OTT services and websites use content delivery networks (CDNs) to deliver their content. CDNs are a network of servers that are distributed around the world. This means that even if the main server for an OTT service or website is blocked, users may still be able to access the content through a CDN server in another region.

v. **Tunneling**: There are a number of tunneling protocols that can be used to bypass internet censorship. These protocols allow users to encrypt their traffic and route it through a different server. This makes it difficult for TSPs to block access to specific websites or OTT services.

vi. **Encrypted Traffic**: Many OTT services and websites use encryption (such as HTTPS) to secure communications between users and their servers. Encrypted traffic makes it challenging to identify and block specific content or services. Only DPI techniques can be used to analyze encrypted traffic and identify specific patterns associated with banned services. However, DPI has its limitations and may face legal and privacy concerns – since communication will essentially have to be intercepted by a TSP in order to conduct a DPI – i.e., examine each packet of data for correctly identifying the OTT service or website that has to be blocked. It is also quite possible that a data packet may contain personal information or sensitive personal data or information (such as financial information). Therefore, investigating each packet of data sent over the internet will have serious privacy and free speech concerns. DPI also raises net neutrality concerns.

vii. **Proxy Servers and VPNs**: Users can circumvent bans by using proxy servers or virtual private networks (VPNs) to access banned OTT services or websites. These tools mask the users actual IP addresses, making it difficult to enforce regional bans effectively. It is always challenging for an ISP to completely block proxy servers and VPNs. Users may also switch to lesser-known OTT services in order to circumvent instances where an OTT service or website is selectively banned.

viii. **Domain Fronting**: Some OTT services and websites use domain fronting, a technique that allows them to appear as legitimate services while communicating with their servers over encrypted channels. Implementing advanced traffic analysis and pattern recognition techniques can help detect and block domain fronting attempts but the same will prove to be very difficult for an ISP, since it may require continuous updates and improvements to stay ahead of new evasion techniques. Such practices of OTT services would make selective blocking redundant.

In addition to these technical challenges, any selective banning framework may face legal or constitutional challenges as well. This is because consumers rely on OTT services to exercise their fundamental rights – including the right to free speech and right to carry on trade – over the internet. Preventing them from accessing the same for certain periods of time may fall afoul of the proportionality principle.[9] One of the criteria to this principle is that the State can curb a fundamental right in order to achieve a legitimate goal. However, the restrictions it introduces in this regard should be absolutely necessary. There should also be no better alternatives to the restriction that is sought to be imposed. At this stage, it is unclear whether selective banning of

[9] Anuradha Bhasin v. Union of India & Ors., W.P. (C) No. 1031 of 2019.

OTT services is the least restrictive option available to the Government to counter public unrest or spread of unlawful activities in specific regions.

Thus, selective banning is not a feasible approach. Moreover, there are various work arounds that exist to circumvent selective banning. IAFI is totally against any selective banning of OTT services.

Q-11. 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.

At the outset, we believe that regulatory authorities should exercise their content takedown powers under applicable laws (for example, under Section 69A read with the Blocking Rules, and Section 79 read with the IT Rules) before considering the option of selectively banning an OTT service. An OTT service ought to be selectively banned only as a last resort, i.e., if it found to be in deliberate non-compliance with applicable laws in India or if it deliberately does not assist law enforcement agencies in tackling the transmission of unlawful content on the internet. In such situations, Section 69A of the IT Act read with the Blocking Rules is sufficient and can be relied on by regulatory authorities (and has been relied on in the past[10]) to block select OTT applications on the grounds enumerated thereunder, including sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order. Further, Section 79 read with the IT Rules can be relied on to block access to online content under certain grounds. Under this law government agencies can also request information from intermediaries for reasons such as identity verification, prevent and detection of crimes, or cybersecurity incidents.

As such, there is no 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. The current legal framework is sufficient to deal with bad actors operating on online platforms, rather than adversely affecting all users' rights to access these online services.

Q-12. 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.

[10] 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

We reiterate that there is no need to implement a regulatory framework for selective banning of OTT services or websites in the country (as explained in Question 11 above). Thus, we have not provided our inputs to this question.

Q-13. 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 reiterate that there is no need to implement a regulatory framework for selective banning of OTT services or websites in the country (as explained in Question 11 above). Thus, we have not provided our inputs to this question.

We reiterate that the IAFI is against any selective banning.

Q-14. 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.

Please note that we have provided all our comments and suggestions in relation to the questions posed in the Consultation Paper and we request you to refer to the same. In particular, please refer to our responses to Questions 5, 6, 7, 8, 9, 10, and 11 above.

****