Bharti Airtel Ltd.
India & South Asia
Airtel Center, Plot No. 16,
Udyog Vihar, Phase - IV,
Gurugram - 122 015
Haryana, India

www.airtel.in
Call +91 124 4222222
Fax +91 124 4243252

TRAI/FY23-24/33
Dated: 01.09.2023

To,
Shri Akhilesh Kumar Trivedi,
Advisor (Network, Spectrum and Licensing)
Telecom Regulatory Authority of India,
Mahanagar Door Sanchar Bhawan,
JawaharLal Nehru Marg,
New Delhi – 110 002.

Subject: Response to Consultation Paper on "Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services"

Dear Sir,

This is in reference to TRAI's Consultation Paper on "Regulatory Mechanism for Over-The-Top (OTT) Communication Services and Selective Banning of OTT Services" dated 07.07.2023 (CP No. 10/2023).

In this regard, please find enclosed our response for your kind consideration.

Thanking You,

Yours' Sincerely,
For Bharti Airtel Limited

Rahul Vatts
Chief Regulatory Officer

Encl: a.a

Response to TRAI Consultation on *Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*

Preamble:

Airtel would like to begin by thanking the Authority for issuing this important consultation paper that aims to introduce a regulatory framework for the governance of Over-The-Top (OTT) Communication services and discusses issues around their selective banning.

The issues under consultation are critical and would impact not just telecommunications, but also the ways and means by which interpersonal communication is exchanged within the legal and regulatory framework of the country.

Evolution of OTT Services:

In the past decade, there has been an exponential rise in the number of internet subscribers both at national and international level. The increase in broadband subscribers and data consumption has witnessed an increased penetration of OTT services and applications in the country.

OTT services and applications have thrived and multiplied, enabling factors being absence of any regulatory barriers and instant access to a global audience through the broadband connectivity powered internet, a fact noted by the Authority, as well. **As a result of such unfettered access, they have become significant players** in the global as well as national economy.

The global OTT market size reached US$ 150.51 billion in 2021 and is anticipated to increase by around US$ 1241.6 billion by 2030.[1] At the domestic level, the share of India's core digital economy expanded from 5.4% of Gross Value Added (GVA) in 2014 to 8.5% in 2019.[2]

An important area where the impact of digitalisation and OTTs is particularly significant is telecommunications. As per TRAI data, between QE June 2013 and QE December 2022, the number of outgoing SMSes per subscriber per month has declined by ~55% and the number of outgoing ILD voice minutes of usage per wireless subscriber per month fell by 83%. With this decline in traditional voice and SMS traffic, there has been a simultaneous increase in OTT traffic. *A report[3] suggests that OTT traffic had, in fact, overtaken traditional carrier traffic as far back as 2016*.

In the broadcasting sector as well, the popularity of OTT platforms is growing day by day. For instance, the recently concluded Indian Premier League (IPL) 2023 was simultaneously broadcast both on a TV channel and on an OTT platform. Both winners together recorded a viewership of close to 100 million.

Need for Regulating OTT Services:

Ever since the emergence of OTT services, the need for regulating them has remained a critical question.

Various sectoral regulators in India have been proactively keeping track and modifying the regulatory framework to include any OTT players that may be offering services similar to those being offered by the traditional players under their jurisdiction.

---

[1] https://www.precedenceresearch.com/over-the-top-market

[2] RBI's Monthly Bulletin, December 2022 (https://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/0RBIBULLETINDECEMBER2022839AD8E8AE984FA7AEE5F6EE71569DEF.PDF).

[3] See para 2.54 of the extant TRAI CP

Response to TRAI Consultation on *Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*

Regulators like RBI, SEBI, IRDAI etc. have created a virtuous framework in their respective sectors, that allows innovation and the growth of OTTs/online players while simultaneously ensuring legal & regulatory oversight without disrupting the level playing field.

In contrast, thus far, no regulations have been drawn up for OTTs operating in the telecommunications and broadcasting sector and as a result **a non-level playing field has emerged between them and the traditional telecom service providers (TSPs).** TRAI has debated the issue, but no concrete steps have been taken till date. It is thus high time that these services are brought within legal and regulatory framework.

Same Service – Same Rules:

The voice/video calling and messaging services have traditionally been provided only by licensed TSPs – being governed by the licenses granted under the Indian Telegraph Act, 1885. However, the market has undergone a paradigm shift with the IP-fication of network and services layers. Today, these services can be delivered using traditional text messaging and CS voice or packet switched (IP) voice/SMS over a Telco network and, also via a standalone untethered application as a packet switched VoIP/messenger.

1. **The services provided by licensed TSPs and OTT communication services are functionally similar and/or substitutable and offer the same core utility.**

   While there may be a difference in the underlying modes of delivery of OTT communication service using an internet application and a licensed TSP's traditional service, the services are used interchangeably by end users. The core utility of the service remains the same, i.e., exchange of inter-personal communication in real-time with another user. The richness of features or add-ons of an application do not change this.

2. **There has been a regulatory lacuna for OTT communication services.**

   As opposed to traditional licensed TSPs, OTT communication service providers offering these interpersonal communication services are not covered under the extant telecom licensing and regulatory framework. It is submitted that **such services should be governed by the same set of rules irrespective of whether provided by an operator on its own network or through the internet**.

3. **Security, privacy and consumer protection are *sine qua non*.**

   While license conditions ensure that communications exchanged through traditional telecom services can be monitored by law enforcement agencies, the same is not true of **OTT communication services which continue to be unmonitored – hindering the processes of law enforcement and crime prevention.** Similarly, there are checks and balances w.r.t. customer data handled by TSPs, but that is not the case with OTT communication services and this risk is exacerbated manyfold by the fact that most of their servers are located outside India. It is therefore doubly **important that security, privacy and consumer protection measures are horizontally applied across all interpersonal (P2P or business, alike) communication.**

This principle of 'Same Service – Same Rules' is a must to ensure a level playing field and fair competition in the sector.

In this context, we submit that the **Authority shall consider bringing a separate authorisation for OTT communication services under the Unified License (UL),** to balance security & privacy needs and service innovation.

Fair Share:

As the importance of connectivity increases, there is a growing need to adopt new technologies. In order to adopt, integrate and sustain new technologies, massive investments are required in the network infrastructure on a continuous basis. The ongoing 5G rollout requires intense fiberization and densification of antennas, the need for which is only going to increase with the future deployments in 6G (i.e. TeraBit capacities and sub-millisecond latency, answering to future network requirements). These developments will intensify pressure and will have a significant impact on the viability of mobile network operators (MNOs) as well as of other actors in the value chain. Robust telecom and digital infrastructure is essential for realizing the Hon'ble PM's vision of Digital India. In this context is important to reflect on as to how the nation would secure a resilient connectivity architecture based on a sustainable business model.

With CAGR of 53% in MBB data traffic during 2017-22, India's data usage amongst the highest in the world. Data traffic in India jumped 3.2 times in the last five years, reaching over 14 exabytes per month. India also has the one of the lowest Internet data rates in the world. Notably, Indian operators have spent over INR 1.5 lakh crore in the recent spectrum auctions. The 5G networks require up to 3 to 5 times more sites and fiberisation and this means continued capex, which requires the industry's financial health to be sound. India's 5G rollout is among the fastest in the world.

Given the above, there is growing underlying concern for the telecommunications sector on its ability to maintain the pace of investment over the long term and thus the sustainability of the Indian digital ecosystem. The telecom operators are forced to expand and upgrade capacity to meet traffic demand. This translates into higher costs for mobile network operators that cannot be recovered, as increasing investments do not generate additional revenues.

Under these conditions, the telecom sector faces increasing challenges in maintaining the pace of investment and the sustainability of the digital ecosystem. Telecom operators can undertake investments only if they receive fair and proportionate returns on their investments.

Fair Share for telecom networks can be ensured by largest traffic originators (LTOs) paying for the traffic delivery services provided by telecom operators. Supporting sustainability of networks is required to match the demands needs (capacity, quality and coverage).

Any entity which creates a property or infrastructure by investing funds, is entitled to charge (rent /lease charges, etc.) from the user of that property or infrastructure who uses the same for commercial purposes. LTOs continue to gain massive direct / indirect benefits at the expense of TSPs. Therefore, they must reasonably compensate TSPs for using the network established by them.

Given the large requirements for meeting the vision of digital India, large traffic originators that account for a disproportionate amount of these investments must contribute a fair share. This should be through a direct contribution to TSPs.

Response to TRAI Consultation on *Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*

Government needs to provide a legal framework to ensure that large traffic generators pay a fair and proportionate share to network operators for the services provided to them and to incentivize them to deliver the traffic in a more efficient way to ensure economic sustainability of network deployments. The topic being critical for sustainability of industry, the TRAI may even consider initiating a separate and detailed consultation on this issue to decide on modalities of fair share.

Selective Banning of OTT Services and Websites:

While we welcome the suggestion of exploring selective banning of OTT services and websites as an alternative to complete internet shutdowns, we submit that the blocking has to be done at the source level for it to be effective. Even content takedown orders are issued directly to entities hosting the content. Similarly, **the OTT services and the entities hosting the websites purported to be blocked should directly be involved in the blocking as the appropriate stakeholders, instead of relying on TSPs/ISPs**.

Response to TRAI Consultation on *Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*

In summary:

- The definition of OTT services as suggested by OFCOM should be adopted in India as well i.e. *"Over-the-top or OTT services refers to a type of service provided "over the top" of an existing data network connection such as a fixed or wireless broadband connection."*
- Just like financial sector regulators (SEBI, RBI, IRDAI) regulate services in their sectors through online mode or digital platforms, the telecom and broadcasting sector also should have regulatory framework for OTT players offering telecom and broadcasting services.
- OTT services should be classified in three categories i.e.
  - *OTT communication services: Internet Protocol (IP) enabled communications services carried over underlying telecommunication/broadband network infrastructure, such as IP-based instant messages or voice or video calls.*
  - *OTT broadcasting services: OTT services delivering the same content as is being delivered on DTH/IPTV/Cable TV, with minimum lag or marginal changes, through underlying telecommunication/broadband network infrastructure.*
  - *OTT application services: OTT services that do not fall in the above two categories.*
- *Functional similarity and/or substitutability of services of traditional licensed TSPs should be used as the intelligible differentia for the reasonable classification of OTT communication services. Accordingly,* OTT communications services should be classified as:
  - *OTT Communication Services (Main): OTT communication services where inter-personal communication is the principal or independent offering, capable of acting as a functional substitute of the services provided by traditional licensed TSPs.*
  - *OTT Communication Services (Incidental): OTT communication services where inter-personal communication is only an incidental or ancillary feature to the principal offering and does not act as a functional substitute or independent of the services provided by traditional licensed TSPs.*
- The Government shall consider an appropriate regulatory framework for OTT Communications Services (Main) with a separate authorization under the UL.
- The OTT communication service (Main) providers should be responsible for establishing the technical infrastructure required in India for lawful interception and comply with data protection and privacy norms including any specific measures prescribed under the UL.
- Given the large requirements for meeting the vision of digital India, large traffic originators that account for a disproportionate amount of these investments must contribute a fair share. This should be through a direct contribution to TSPs. The topic being critical for sustainability of industry, the TRAI may even consider initiating a separate and detailed consultation on this issue to decide on modalities of fair share.
- The selective banning of websites at the TSP/ISP end would not serve any purpose. The Government should consider source-level blocking, i.e., directly engage with such OTT service providers /website /hosting server / platforms for effective implementation.

With this background, Airtel provides its detailed comments and answers to the specific questions raised by the Authority in the sections that follow.

Response to TRAI Consultation on *Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*

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

Airtel Response:

As discussed in the Preamble, **the services provided by licensed TSPs and OTT communication services are functionally similar and/or substitutable and offer the same core utility.** In order to create an effective regulatory framework, the entities to whom such a framework would apply need to be identified or determined. This means drawing up a clear and specific definition of 'OTT services'.

With no regulatory oversight up until now, a universally accepted definition of 'OTT services' does not currently exist in India. While some may understand it only to mean video streaming platforms such as Netflix or Hotstar, the scope of 'OTT services' is actually much wider from a technological point of view. Applications and services running over the internet, not requiring any separate network or infrastructure, can be said to be running on top of the data connectivity provided by telecom networks and hence classified as an 'OTT service'.

Thus, digital services – ranging from video-on-demand (Netflix, Amazon Prime, etc.), audio streaming (Spotify, etc.), email (Hotmail, etc.), instant messaging (WhatsApp, Telegram, etc.), social media (Facebook, Instagram, etc.) to payment gateways (Paytm, etc.), e-commerce (Amazon, Flipkart, etc.), food ordering (Swiggy, Zomato, etc.), online gaming (PUBG, Among Us, etc.), online dating (Tinder, Hinge, etc.), and much more – are all OTT services.

Considering this, Airtel is of the view that the definition of over-the-top (OTT) services as suggested by OFCOM should be adopted in India as well:

> "***Over-the-top or OTT services*** *refers to a type of service provided "over the top" of an existing data network connection such as a fixed or wireless broadband connection."*

Airtel believes that the above definition adequately captures the wide variety of services that run "over-the-top" of data/traditional telecom services.

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.

Airtel Response:

Please refer to the Preamble and the response to Q1.

'OTT services', an umbrella term, covers an extensive range of online services and applications, with the utility/functionality of one set of services being wholly different from another set or similar in same category/class, both within the umbrella.

Therefore, it would not be prudent to apply one blanket set of rules and regulations to several different kinds of OTT services. It is important to classify them into different categories so that appropriate regulatory frameworks may be devised for each category.

In this background, various sectoral regulators have been proactively keeping track and modifying the regulatory framework to include any OTT players that may be offering services similar to those being offered by the traditional players under their jurisdiction.

For instance, **Reserve Bank of India (RBI) came out with 'Guidelines on Digital Lending' last year to allow fintech/ digital platforms i.e., non-regulated entities to offer loans only after partnering with a bank/NBFC i.e., regulated entity permitted to carry out lending activities.** Under the Guidelines, all loan disbursals and repayments are required to be executed only between the bank accounts of borrower and the Regulated Entities without any pass- through/ pool account of any fintech or third party. The intent of the Guidelines was to protect the integrity of the banking system against entities that are not regulated and not authorized to carry out lending business, while ensuring ways to reap the benefits of digital innovation at the same time. The Guidelines set up an institutional mechanism to ensure orderly growth of the sector, preserving financing stability and protection of data privacy.

Similarly, wealth/asset management services are increasingly provided online now – people can invest in stocks, mutual funds, etc. with a click on their phones. **The Securities Exchange Board of India (SEBI),** the stock market regulator now oversees the digital platforms providing stock broking and mutual fund manager services.

The Insurance Regulatory and Development Authority of India (IRDAI) monitors insurance services irrespective of the mode in which they are provided, i.e., offline or online by whichever player. Specifically, it has issued clear guidelines for the online sale and servicing of insurance policies.

Another sector worth paying attention to is **consumer goods retailing**. Earlier, a person had to visit a physical shop or market to buy something. Now, anything and everything, from daily essentials like groceries to precious goods like jewellery can be ordered online. These e-commerce platforms and applications have also **been brought within the ambit of the Consumer Protection Act**.

Recently, **the Ministry of Electronics and Information Technology (MeitY)** amended the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 for setting out the guidelines for online gaming.

The above approaches highlight the importance of sound regulatory frameworks as the regulators in these critical sectors have not left the OTTs/digital platforms unattended to operate in the formers' sectoral service domains without any oversight.

However, the telecom and broadcasting sector is an outlier to the extent that there is no regulatory oversight by TRAI/DoT/MIB on the OTT players offering telecom and broadcasting services, even though they are significant players in the market as outlined above. Airtel believes that this situation needs to be corrected immediately. That said, while categorising OTT services into different groups for the purpose of regulation, it needs to be kept in mind what kind of services are being offered by OTT players vis-à-vis traditionally licensed/regulated players.

As an illustration, some video streaming platforms offer the same content as available on satellite TV channels with marginal changes or minimal lag, and thus compete with traditional distributors, i.e.,

DTH/HITS/IPTV/Cable operators – requiring the application of 'same service – same rules' principle, in order to quell any level playing field concerns. On the other hand, some video streaming platforms do not offer any live linear TV content, and thus do not compete with traditional distributors. Therefore, it is only appropriate that these two kinds of video streaming platforms are classified into separate categories, in order to ensure the application of suitable rules to each category.

Thus, **the type of service being offered to the customers should be used as the intelligible differentia for the reasonable classification of OTT services**, so that appropriate rules can be applied to specific services and a level playing field can be maintained vis-à-vis the traditional players.

Classification of OTT Services:
Based on the above criteria, the relevant categories of OTT services would be as follows:

1. OTT communication services: Internet Protocol (IP) enabled communications services carried over underlying telecommunication/broadband network infrastructure, such as IP-based instant messages or voice or video calls.

   The OTT services, which offer same/similar services compared to traditional telecom services, would be covered in this category. Some examples of such services would be WhatsApp, Telegram, etc.

2. OTT broadcasting services: OTT services delivering the same content as is being delivered on DTH/IPTV/Cable TV, with minimum lag or marginal changes, through underlying telecommunication/broadband network infrastructure.

   The OTT services, which offer same/similar services compared to services of traditional distributors of TV channels, would be covered in this category.

3. OTT application services: All OTT services which do not fall into the above two categories.

   The OTT services, which do not need any regulation from the perspective of TRAI would be covered in this category.

The above classification is in the specific context of the telecom and broadcasting sector, since other regulators like RBI, SEBI, etc. are framing the rules for OTT players operating in their respective sectors.

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.

Airtel Response:

Please refer to the Preamble and the response to Q2.

Today, voice and SMS communications services can be delivered using traditional text messaging and CS voice or packet switched (IP) voice / SMS over a Telco network. They can also be delivered via a standalone, untethered application as a packet-switched VoIP /messenger. This transformation has

come about because of the significant IP-ification of network and services layers. The regulatory regime should be future fit to accommodate such changes impacting service delivery and regulate them appropriately, just as they may have to adjust to a time when quantum technologies become mainstream and the same voice/video/messaging services are delivered using them maybe in a different form.

Airtel believes that functional similarity and/or substitutability, especially demand-side substitutability, should be main parameters for classifying any service as an OTT communication service.

OTT communication services which are similar to access services (such as collection, carriage, transmission and delivery of voice and/or non-voice messages), internet telephony, services including IPTV, triple play, i.e., voice, video and data, voice mail, unified messaging services, video conferencing, cell broadcast, value-added services and supplementary services, provided by traditional licensed TSPs, should be considered under this definition. Same/similar services should also cover services that will potentially be provided by TSPs in the future, as permissible under their licenses.

Thus, the definition of OTT communication services needs to **be future agnostic and must cover all such services that may substitute or supplement telecom services as permitted to licensed telecom operators** under license conditions. Also, it should be flexible and periodically reviewed based on the evolution of the market structure, technological developments, innovations and the extent of substitutability created by such services.

Accordingly, the definition of OTT communication services should be as follows:

> "***Over-the-top or OTT communication services*** *means Internet Protocol (IP) enabled communications services carried over underlying telecommunication/ broadband network infrastructure such as IP based instant messages or voice or video calls.*"

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.

Airtel Response:

Please refer to Preamble and the response to Q3.

The definition of 'OTT communication services' proposed earlier covers all OTT services which allow inter-personal communication – whether voice-based or video-based or messaging-based. The ability to carry out this communication exchange in real-time with minimum lag/latency should have no bearing on classifying these as OTT communication services.

There are some OTT services where inter-personal communication is the ***main*** offering (like WhatsApp and Telegram), and there are some OTT services where the inter-personal communication facility is only an ***incidental or ancillary*** feature and intricately linked to a different principal service (like Zomato and Uber).

Both these kinds of services would technically come under the definition of 'OTT communication services'. However, while the former can act as, and in fact do act as, functional substitutes of the services provided by traditional licensed TSPs, the latter do not.

Accordingly, **functional similarity and/or substitutability of services of traditional licensed TSPs should be used as the intelligible differentia for the reasonable classification of OTT communication services**. Based on the above criteria, the relevant categories of OTT communication services would be as follows:

1. OTT Communication Services (***Main***): OTT communication services where inter-personal communication is the principal or independent offering, capable of acting as a functional substitute of the services provided by traditional licensed TSPs.

   For instance, the principal offering on WhatsApp and Telegram is inter-personal communication and they have already become effective substitutes of the services provided by traditional licensed TSPs around the world, as suggested by various statistics.[4]

   The principle of 'same service – same rules' needs to be applied in case of such OTT communication services vis-à-vis traditional licensed telecom services.

   Such OTT communications services should be considered under the Unified License.

2. OTT Communication Services (***Incidental)***: OTT communication services where inter-personal communication is **only an incidental or ancillary feature** to the principal offering **and does not act** as a functional **substitute** or independent of the services provided by traditional licensed TSPs.

   In these services, the inter-personal communication feature is so intrinsically linked to the principal service that it cannot technically be used without that principal service. The users cannot choose to communicate with a person of their choice – the users are assigned to each other for a particular task and once the same is completed, it is usually not possible to communicate with the same person again.

   For instance, on Zomato and Uber, a customer can only communicate with the particular delivery executive or driver assigned for their order delivery or cab ride, respectively, for that particular delivery or ride. Once the order is delivered or the cab ride has ended, it is not possible to communicate with that particular person again.

   However, there can be a sub-category of incidental OTT communication services that may (actually) fall under OTT communications services (Main). For example, Instagram, principally a social media platform, also offers instant messaging/voice/video calling features which are independent of the social media offering, i.e., one does not need to mandatorily create a social media post in order to be able to communicate with other users. Similarly, on Paytm, although

[4] The user base of WhatsApp in India stands at 487 million – the highest in the world, and this number is growing at a rate of 16.6% every year. WhatsApp users globally make about 2 million voice and video calls on an average daily. (https://verloop.io/blog/whatsapp-statistics-2023/#:~:text=India%20has%20the%20most%20WhatsApp,rate%20of%2016.6%25%20every%20year)

the principal offering is financial services, an instant messaging feature which is independent of the financial services is also offered, i.e., one does not need to mandatorily carry out a financial transaction in order to be able to chat with other users or users unrelated to the financial transaction.

It may be noted that even the European Electronic Communications Code makes a similar differentiation between Main and Incidental OTT communication services. It further states that the words 'incidental' and 'ancillary' should be interpreted narrowly and from an objective end-user's perspective. Airtel endorses the same for the Indian context as well.

Therefore, the Government shall consider bringing The OTT communications service (Main) being completely substitutable, - under the UL authorization.

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.

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.

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.

Airtel Response:

Please refer to the Preamble and responses to Q1-Q4.

Response to TRAI Consultation on *Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*

Airtel believes that all types of **OTT communication services should be brought under the appropriate regulatory framework.** The functionality of the service and the utility and/or substitutability of services from a customer's standpoint – irrespective of the underlying technology/resources being used by the operator for the provision of such services – is what should govern the remit of the regulatory and licensing framework between TSPs and OTT communication service providers.

Therefore, the principle of 'same service, same rules' needs to be applied so as to address the glaring licensing, regulatory and security asymmetries between two sets of services to ensure a level playing field and to protect competition.

Our views on the various aspects of OTT communication services vis-à-vis licensed telecommunication services in India are as follows:

(a) Regulatory aspects:

As per the Indian Telegraph Act, various national telecom policies and the present licensing regime, the privilege to offer interpersonal communication services is to be given by entities holding the license granted under section 4 of the Indian Telegraph Act. These licenses impose numerous conditions on the licensees – **lawful interception, subscriber verification, protection of customer privacy, network security, maintenance of CDR, emergency services, etc. –discussed in detail in the sections below**. These requirements are enshrined to secure and protect the critical network infrastructure, communications and consumer – and are of immense importance to nation's economic, strategic and social interests, and the consumer at large.

The licensees are subject to multiple regulatory fees and levies such as a one-time non-refundable entry fee, annual license fee (LF) of 8% (this includes a USO levy of 5%) and in case of spectrum, spectrum-related payments and charges.

The licensees also have to comply with the various regulations, orders and directions issued by TRAI from time to time. Some of the key regulations relate to interconnection, quality of service, consumer grievance redressal, mobile number portability, curbing unsolicited commercial communication (UCC), tariff protection, metering and billing accuracy, etc.

As for **OTT communication services, they are real time, inter-personal (person-to-person or business, alike) telecommunications services**. They are almost the same or, at any rate, very similar to the telecommunications services provided by licensed TSPs except that instead of providing these services through their own networks, OTT communication service providers provide these services over the internet using Telco connectivity.

While the layer being used by the two kinds of operators may be different, the services offered by the OTT communication service providers are substitutes – from a customer's standpoint – for the services offered by licensed TSPs. Even the TSPs' voice service today is carried over IP protocols though not necessarily as a separate app.

The important point here is that unlike the traditional licensed TSPs, OTT communication service providers are being allowed to offer these services even though they do not hold a telecom license in India. What is more, they are not being made subject to any of the rules and regulations the TSPs have had to abide by. This has been observed by the Authority itself in paras 2.66 to para 2.72 of the Consultation Paper and has been succinctly summarised in the table under para 2.72.

This, in Airtel's view, amounts to circumvention of the Indian telecom licensing and regulatory norms and should not be allowed to continue. Therefore, OTT communication services need to be brought within a licensing/ regulatory framework forthwith.

Some international examples in this regard have been noted in the Consultation Paper itself. The European Electronic Communications Code adopted by the EU has classified OTT communication service providers into number-based (like VoIP) and number-independent (like instant messaging) service providers. While the number-based services are subject to the same rules as traditional TSPs, a lighter regime is in place for number-independent services.

Singapore requires OTT communication service providers to obtain a Service-Based Operating License that prescribes some minimum QoS standards. Regulation of OTT players is also under consideration in **Trinidad and Tobago**. In **Turkey,** the ICT Authority has been explicitly empowered to regulate OTT service providers through an amendment in 2022, and the issue is being closely monitored by it. **Zimbabwe** has proposed to move to a converged licensing framework, which would also cover OTT service providers.

Coming to India, over the past few decades, the licensing regime has been modified multiple times as per the requirements of the time. It has advanced from standalone licenses for each type of service to a Unified License with separate service authorisations. New licenses and authorisations have been introduced in order to accommodate the new services that have evolved due to technological developments from time to time.

Even after unification, the licensing regime is sufficiently flexible to allow for differential terms and conditions for different service authorisations. In fact, just recently TRAI has recommended a separate authorisation under UL for a new category of *Digital Connectivity Infrastructure Providers (DCIPs)* with zero LF. The M2M services have also been allowed as a separate authorisation under the UL.

In view of the above, Airtel **proposes that a suitable regulatory framework should be introduced for providing OTT Communication Services.** This will ensure that critical issues like security and privacy are taken care of, and technological innovation in the sector is also not hindered.

The OTT communications service (Main) being completely substitutable should be considered to be brought under the UL authorization.

(b) <u>Economic aspects:</u>

With a CAGR of 53% in MBB data traffic during 2017-22, India's data usage was amongst the highest in the world. Data traffic in India has jumped 3.2x in the last five years, reaching over 14 exabytes per month.[5] Indians consume ~ 20GB data per month on average. This is expected to reach 46GB by 2027. Further, India has one of the lowest internet data rates in the world.[6]

The increase in mobile data consumption coincides with the launch of commercial 5G services in the country in October 2022. Notably, Indian operators have spent over INR 1.5 lakh crore in the recent

[5] Nokia Mobile Broadband Index (MBiT) Report (2022); An exabyte is equal to a million gigabytes. Pan-India mobile data usage per month has grown from 4.5 exabytes in 2018 to 14.4 exabytes in 2022.
[6] Worldwide Mobile Data Pricing (2022); India has the fifth lowest Internet data rates in the world. Average price of one gigabyte data in India is $0.17 (around INR 13.50).

spectrum auctions. 5G networks require up to 3x to 5x more sites and fiberisation. India's 5G rollout is among the fastest in the world. It all means more continued capex.

The telecom sector operates face increasing challenges in maintaining the pace of investment and the sustainability of networks. Specially, in comparison to telcos globally, the return on capital employed (ROCE) for operators in India is not even 30% of the weighted average cost of capital (WACC).[7] The creation of digital telecom infrastructure is becoming tougher with rapid data usage and sustainability issues need to be addressed.

Given the large requirements for meeting the vision of digital India, large traffic originators that account for a disproportionate amount of these investments must contribute a fair share. This should be through a direct contribution to TSPs.

(c) <u>Security aspects/ Lawful Interception:</u>

The security and integrity of communications networks and communications itself is of immense importance to a nation's economic infrastructure, strategic interests and social order. It cannot be allowed to be compromised in any manner. Law enforcement agencies and national security agencies need to be provided access to communications networks and data regarding communications flow to protect the larger public interest.

The powers to lawfully intercept and monitor communications are derived from section 5 of the Indian Telegraph Act, 1885. Such powers can be invoked on occurrence of any public emergency or in the interest of public safety or the interests of the sovereignty and integrity of the nation, the security of State, friendly relations with foreign states, public order or for preventing incitement to the commission of an offence. Rule 419A of the Indian Telegraph Rules, 1951, lays down the procedural requirements for lawful interception and monitoring.

The terms and conditions of the license granted to telecom and internet service providers form the next layer of the legal framework for national security considerations. Some of these terms and conditions are listed below:

- Domestic traffic to stay within India.
- Network to be set up within service area or in the country.
- Provision of lawful interception to the security agencies.
- Access of subscriber database to the security agencies.
- Maintenance of CDR/IPDR for various security requirements.

Meanwhile, in direct contravention of all this care for security, OTT communication service providers have transferred the ability to lawfully intercept traffic moving over networks away from constitutionally governed, democratically established and accountable governments to private companies providing such services. They offer calls across telecom networks in India using strong encryption and switching servers located outside the country and hence effectively prevent any lawful interception and/or monitoring of calls handled in their switching servers/network.

These players avoid sharing subscription details of customers and/or logs of communications. In fact, some OTT communication service providers facilitate spoofing of CLI, which makes it difficult to

[7] Barclays (June 2022).

identify or locate the actual caller. Such features enable the use of OTT communication services for the purposes of facilitating/coordinating terrorist attacks, financial corruption as well as various other criminal activities.

Moreover, while the mobile/broadband customers are verified by TSPs, the OTT communication services are offered in such an untethered manner that the identity of the customer of OTT communication services could well differ from the identity of the mobile/ broadband customer. KYC details are also either maintained outside the country or, indeed, not even obtained by the service provider. Due to the untethered nature of the OTT communication services, the KYC details obtained by the TSPs may not match with the actual users in a number of cases.

The security concerns posed by these services were recognised by the Indian Government as far back as 2010, when Blackberry was asked to install a server in India in order to enable law enforcement agencies to monitor its messenger and enterprise mail service.[8]

More recently, national security agencies and the DoT have indicated that VoIP traffic offered by OTT communication service providers be duly intercepted. However, almost all OTT communication service providers deploy strong encryption and the switching and other infrastructure used by these OTT communication service providers is installed outside the country. And, because of this, the unencrypted content can only be intercepted in the switching systems installed outside the country and the encrypted content can only be decrypted outside the country. Since the TSPs merely provide internet and the switching servers are also not under their control, the systems deployed by them are unable to intercept and monitor such strongly encrypted content.

Even the DoT Committee Report on Net Neutrality (May 2015) acknowledged the paramount nature of national security and the risks to national security posed by OTT communication services. Accordingly, it recommended inter-ministerial consultations to work out measures to ensure compliance of security related requirements from OTT service providers.

Besides national security concerns, Indian TSPs also continue to risk violations of their licensing conditions, specifically the condition that mandates them to provide for lawful interception and monitoring of each type of service/product including internet/internet telephony passing through their networks.

It is to be noted here that the European Electronic Communications Code distinguishes between number-based and number-independent services provided by OTT communication service providers. While the number-independent services enjoy a lighter regime, the provisions in respect of security remain the same as traditional licensed TSPs for both number-based and number-independent services, as noted by the Authority itself in the Consultation Paper. The Code has been adopted and enacted into national laws by multiple countries within the EU – Austria, France, Germany, Italy, Finland and Denmark.

However, we would like to highlight that OTT communications services typically leverage the strength of) telecom resource implicitly e.g., voice, video and messaging OTT services (implicitly) make use of a telecom resource (e.g., numbering or a KYCed customer) to successfully enable interpersonal communication. This important consideration should also guide the regulatory framework.

[8] https://timesofindia.indiatimes.com/business/india-business/install-server-or-close-messenger-govt-tells-blackberry/articleshow/6392947.cms?from=mdr

Therefore, **OTT communication service providers should be held responsible for establishing the technical infrastructure required in India for lawful interception, so that national security agencies may intercept their traffic as per requirement**.

(d) Privacy aspects:

The Indian Telegraph Act, 1885, affords protection to users of telecommunication services from unlawful or unauthorised interception. In furtherance of the same, the terms of the license agreement require TSPs to ensure that the privacy of communications is protected.

In the Internet services sector, TSPs, OTT communication service providers, content providers, equipment/handset manufacturers, entities dealing with smartphone operating systems, and browsers, etc. operate in the same internet ecosystem. In this sector, customer privacy has three significant sources of vulnerability – device, network and content providers. All three of these vulnerabilities need to be plugged in order to holistically address the issue of the protection and privacy of personal data.

However, the privacy protection requirements applicable to TSPs are not applicable to the OTT Communications service providers even though they deal with the same personal data of subscribers.

For instance**, while TSPs are not allowed to send the personal data of their customers outside India, there is no such prohibition/restriction on other OTT players**. In fact, in most cases, the personal data being handled by these players resides outside of India. There is no legal provision to monitor or enforce in case of a breach or suspected breach of trust in data protection by these other players – the only instrument available is reliance on their statements.

The Authority itself recognised the inadequacy of the extant framework in its Recommendations dated 16.07.2018 on "Privacy, Security and Ownership of the Data in the Telecom Sector" and recommended that to protect telecom consumers against the misuse of their personal data by the broad range of data controllers and processors in the digital ecosystem, all entities in the digital ecosystem which control or process their personal data should be brought under a data protection framework.

Taking note of the critical nature of the issue, the Authority also recommended interim measures, i.e., till such time as a general data protection law can be notified by the Government, the existing rules/license conditions applicable to TSPs for protection of users' privacy should be made applicable to all the entities in the digital ecosystem.

Thus, **in line with TRAI's recommendations, Airtel submits that OTT communication service providers should be required to comply with the various data protection and privacy norms including any specific measures prescribed under the UL**.

(e) Quality of service aspects:

TSPs are required to comply with various customer-centric regulations issued by TRAI related to quality of service, like minimum QoS benchmarks, metering and billing audits, etc. Although the same QoS norms cannot be made applicable to OTT communication service providers, it is important to

acknowledge that OTT service providers are capable of affecting the TSPs' ability to meet the benchmarks set for them.

The network is getting choked with ever-increasing high bandwidth usage by services such as HD videos, movie streaming, high quality web conferencing, etc. creating challenges for traditional licensed TSPs. They constantly struggle to add capacity to their networks to match the volume and velocity of increase in internet traffic.

This issue came to the fore and was acknowledged by the OTT service providers themselves during the COVID lockdown when they restricted the quality of content to SD, in order to ease the pressure on cellular networks.

Thus, a balanced view needs to be adopted.

(f) Consumer grievance redressal aspects:

Licensed TSPs are mandated to establish an effective consumer grievance redressal mechanism whereby consumers register complaints regarding the services received by them and these complaints need to be resolved within certain prescribed timelines as per TRAI's regulations. However, this is not required of OTT communication services.

It is understood that a lot of OTT communication service providers do have their own policies and mechanisms for consumer grievance redressal. However, in the absence of any mandatory requirements, these mechanisms might not be very effective and user-friendly or transparently known. This may leave consumers with no real avenue to ensure that their complaints are being heard and acted upon.

Thus, **in order to protect the interests of the consumers, OTT communication service providers should be required to set up a consumer grievance redressal mechanism with clear timelines for resolution of issues in a standardised format.**

(g) Other aspects:

Currently, all the traditional licensed TSPs are enabling emergency services to their customers by provisioning these services through state agencies or under agreement with BSNL. In order to enable such services, the TSPs are required to invest in the provisioning of voice, SMS and Location Based services at Emergency Response Support System locations, apart from making payments to BSNL for access to voice services for emergency L-1 codes.

However, OTT communication service providers are not required to provide any such emergency services. Since these services play a crucial role in times of natural disasters, accidents and other emergencies, it is important that **OTT communication service providers also be made liable to provide emergency and public utility services similar to TSPs for the benefit of customers.**

Considering the widespread use of various OTT communication services today, they can be effectively leveraged in cases of emergencies.

(h) Eligibility Conditions/ Financial Conditions (such as application processing fee, entry fee, license fee, bank guarantees, etc.):

Response to TRAI Consultation on *Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*

Airtel believes that the Government should create a regulatory framework which creates a level playing field as well as address the concerns of security and privacy. Such a regime should also ensure that there is no hindrance to technological advancements and innovation in the sector and not burden them.

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.

Airtel Response:

Yes, there is a need for a collaborative framework between OTT communication service providers and licensed telecommunication service providers. To understand its need, we first explain the dynamics influencing the telecom and OTT ecosystem.

a. Internet traffic is growing rapidly.

- Internet traffic is expanding rapidly, by 35% per year and more than 50% for mobile data.
- Only a handful of large global digital platforms drive this growth, generating more than half of the total Internet traffic.
- India's data usage amongst highest in world; CAGR of 53% in MBB data traffic during 2017-22.
- Data traffic in India jumped 3.2x in last five years, reaching over 14 exabytes per month.
- Indians consume nearly 20GB data per month, and this is expected to reach 46GB by 2027.
- As a result, TSPs forced to continuously expand & upgrade capacity to meet traffic demand.

b. Investment needs for 5G

- Increase in mobile data consumption coincides with launch of 5G in the country in.
- Indian operators have spent over INR 1.5 lakh crore in the recent spectrum auctions.
- 5G networks require up to 3 to 5 times more sites and fiberisation and this means continued capex, which requires the industry's financial health to be sound.
- India's 5G rollout is among the fastest in the world.
- This translates into higher costs for TSPs that cannot be recovered, as increasing investments do not generate additional revenues.

Presently only telecom operators are bearing the cost of the necessary investments in infrastructure, in an increasing unsustainable market, while the other side of the market, the large traffic generators (LTGs) or content providers, are benefiting from the network, without contributing for the service received. As a result, many TSPs now have returns on investment below their cost of capital. And due to bargaining asymmetry and market power, TSPs cannot get large traffic originators to pay for the service. Under these conditions, the telecom sector faces increasing challenges in maintaining the pace of investment and the sustainability of the digital ecosystem.

With the launch of 5G and a newer generation of bandwidth-hungry applications and services to come in the future as well, the need for creating appropriate mechanisms and managing the contribution of

stakeholders towards the creation of digital infrastructure needs to be deliberated. This requires a fair contribution by all stakeholders in larger digital ecosystem.

The thought of fair and equitable contributions from all such stakeholders who contribute towards creating traffic and thus impact network investments and capacities is gaining currency every day, e.g., in both Europe and the US.

Given the large requirements for meeting the vision of digital India, large traffic originators that account for a disproportionate amount of these investments must contribute a fair share. This should be through a direct contribution to TSPs.

There should be an enabling provision that allows the Government to direct such stakeholders to make payment, as maybe prescribed, as their share of contribution to the capital cost of broadband networks. This may be computed basis traffic, revenue, number of consumers or some other parameter that should be decided soon.

We recommend traffic on network as the parameter. The objectives of such framework should be to ensure that only the large traffic originators, those exceeding a 5% bandwidth occupation at peak hours[9] measured at individual operator network level, who impact substantially on operators' networks, fall within its scope and make a fair share to the costs of network infrastructure, thus protecting innovation and allowing smaller OTTs to thrive and compete.

The Fair Share solution aims to restore the balance of the digital ecosystem to ensure the sustainability of networks, benefiting both telecom operators and large digital platforms. The topic being critical for sustainability of industry, the TRAI may even consider initiating a separate and detailed consultation on this issue to decide on modalities of fair share.

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.

Airtel Response:

We do not foresee any potential challenges that may arise out of a collaborative framework. Rather, we believe that a legislative / regulatory framework that allows fair contribution towards creation of digital connectivity infrastructure, will help address the sustainable investment challenges that the industry faces.

We submit the following w.r.t certain aspects which may be seen as a concern area, but in our considered view, will have no such issue if a regulated collaborative framework is put together between OTT communication providers and telecom providers.

(a) Net neutrality

i. The fair share proposal is fully compliant with net neutrality obligations.
ii. Any collaborative framework for fair contribution between OTT and licensed TSPs will not affect access to an open and free Internet.

[9] Busy/Peak hour is defined as 60 minute period of highest bandwidth usage within a week. Provided data average of one year (52 weeks).

iii. Need for *systemic traffic generators* to contribute fairly to network deployment has nothing to do with the net neutrality debate. It does not involve anyhow a differentiated traffic management or unequal treatment of LTGs traffic.
iv. Net Neutrality does not prohibit charging LTGs for the service they receive, provided that such agreements and commercial practices do not limit the exercise of the rights provided for in the Regulation.
v. Content and services will remain fully accessible with no traffic management/ differentiation implemented. There will be no throttling, no blocking, and no paid prioritization.
vi. There is no violation of net neutrality if a peering charge is applied at an interconnection point between two networks to compensate for an imbalance of data traffic. This charge is applied in relation to the volume of the traffic and not for certain data from certain OTT.
vii. Such interconnection peering charge has no influence on the access of end customers to any content. Thus, network neutrality would not be at stake in this situation.
viii. The price for the traffic paid by end users will not change depending on whether the traffic originator is subject to fair share payments or not.
ix. By defining a threshold to be subject to the obligation, only largest traffic originators will have to pay for the service of delivering their traffic to end users.

(b) Consumer Interest and Choice

i. A collaborative framework for fair share will benefit all – end customers, MNOs and OTT service providers, by ensuring the deployment of faster high-capacity networks with the required quality and with innovative services.
ii. An efficient and fair cost-sharing policy restricted to only largest traffic originators will ensure a better quality of service for users and a faster roll-out.
iii. A fairer allocation of network costs can relieve the pressure on consumer prices for communication services as the only way to meet investment needs.
iv. A better deal for consumers, as today their internet bills effectively cross-subsidize the revenue models of large traffic generators.
v. Gains in network quality, resulting in improved users' online experience. Telehealth, online education, expansion of hybrid working, new applications, such as the Metaverse, and mission critical services all require reliable internet connections. It seeks to ensure advanced connectivity and benefits for citizens and businesses, with the aim of improving the future quality of life.

(c) Impact on innovation and on Start-ups

i. By defining a threshold, only the biggest traffic generators will have to enter direct collaborative framework with telcos. Only those companies enjoying asymmetric bargaining and market power will be covered under the scope.
ii. This will not impact smaller OTTs, SMEs and startups and would thus be not detrimental to innovation as alleged.
iii. LTGs can be designated on quantifiable criteria like - size, volume of traffic, turnover threshold, number of users or other criteria.
iv. Direct collaboration is the most credible and practicable solution, which requires only a few LTOs account for over 50% of total global data traffic, to share the cost of delivering the traffic.

The Fair Share solution aims to restore the balance of the digital ecosystem to ensure the sustainability of networks, benefiting both telecom operators and large digital platforms. The topic being critical for

sustainability of industry, the TRAI may even consider initiating a separate and detailed consultation on this issue to decide on modalities of fair share.

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.

Airtel Response:

Under the provisions of the Indian Telegraph Act and the *Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017,* the Government is empowered to order temporary suspension of telecom services on the grounds of public emergency and public safety. These provisions are frequently invoked, and TSPs/ISPs are directed to shut down internet services in specific areas, in order to bring emergency situations under control as well as for preventative purposes.

However, even though the main purpose usually is to control the spread of hate speech/ misinformation/ disinformation through OTT communication services and social media platforms, the whole of the internet is shutdown – leading to the denial of even critical or essential services like telemedicine, digital payments, educations, etc.

Considering the impact of data barring orders on the everyday lives of people, the economy and TSPs, Airtel completely agrees with the Parliament's Standing Committee on Communication and Information Technology, which has suggested that alternative measures need to be explored. One of the alternatives suggested by the Parliamentary Committee is the selective banning of OTT services and websites.

Airtel submits that if the approach of blocking of OTT services/websites through TSPs/ISPs is continued with, several technical challenges will continue to persist – irrespective of the requirement of selective banning of specific OTT services and websites in specific regions of the country for a specific period or otherwise.

Here is a list of some of these:

i. **No network-level differentiation among various OTT services/websites:** On the network front, all OTT services and websites work over Internet Protocol (IP) addresses. An IP address enables a device to send or receive data packets across the internet. Further, in order to protect the privacy and integrity of the exchanged data while it is in transit, the data sent and received across IP addresses involves secured protocols such as HTTPS (Hypertext Transfer Protocol Secure).

   Thus, it is not possible at the network level to detect the type of communication being transmitted and categorise it among social media, video, audio, gaming, file sharing, etc. The network only understands the IP while sending and receiving data over the internet. Further, there is no inventory/repository of the complete list of OTT services and websites along with their respective IP addresses.

   Due to this limitation, there is no solution available to block any specific type of OTT services or websites such as social media apps/websites.

ii. **Dynamic IP Addresses**: OTT services and websites are often hosted on servers with dynamic IP addresses. This means that the IP address of the server can change frequently, making it difficult to trace and/or block access to the service or website. Implementing a dynamic block-list which is updated in real-time, based on domain name system (DNS) queries raised by TSPs/ISPs, will always be a challenge.

This may lead to the blocking of URLs not intended to be blocked, and of the URLs which were actually targeted for blocking working normally due to the change in IP address.

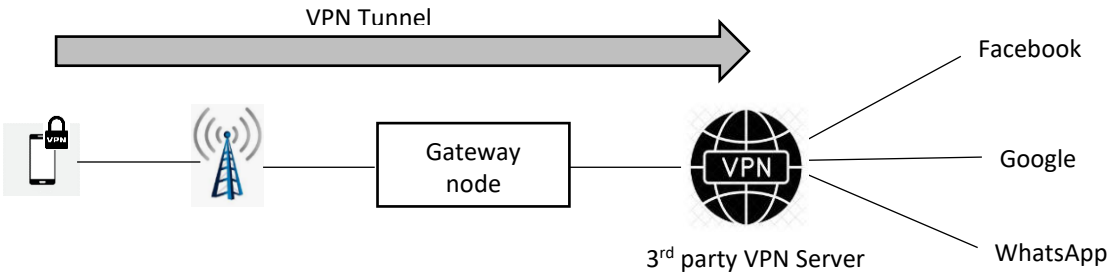
iii. **Inadequacy of Blocking Solutions:** The URL blocking solutions currently available only support TCP based communication. The URL hosting services using QUIC protocol, which in turn leverage UDP in the transport layer, cannot be blocked by such solutions.

Moreover, even in cases of HTTPS protocol, while the main URL of a website is blocked, the sub-URLs/sub-pages of that website can still be accessed by the users.

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, Proxy Servers and VPNs**: There are several 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 censors to block access to specific websites or services.

For instance, users can circumvent bans by using virtual private networks (VPNs) and proxy servers to access banned OTT services. A VPN connection establishes a secure connection between a user and the internet. Via the VPN, all the data traffic generated by the user is routed through an encrypted virtual tunnel. This disguises the IP address when the user accesses the internet.



As long as the data services are not barred, a user can always use these tools to mask the users' actual IP addresses. This would make it difficult to enforce regional bans effectively.

Further, there are a huge number of VPNs hosted across the globe and the list is growing on a daily basis. There is no governing body at the national or international level, which captures or maintains the complete list of VPN IPs. Thus, it is even more challenging for a TSP/ISP to completely block proxy servers and VPNs.

Blocking of specific OTT services/websites will promote the use of VPNs and make it near impossible to trace/track users.

vi. **Encrypted Traffic**: Many OTT services and websites use encryption (such as HTTPS) to secure communication between users and their servers. Encrypted traffic makes it challenging to identify and block specific content or services. Only Deep Packet Inspection (DPI) techniques can be used to analyse encrypted traffic and identify specific patterns associated with banned services. However, DPI has its limitations and may face legal and privacy concerns. It is also quite possible that the packet may contain financial information.

vii. **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 that can help detect and block domain fronting attempts is very difficult for a TSP/ISP, it requires continuous updates and improvements to stay ahead of new evasion techniques.

viii. **Over-blocking and Collateral Damage**: Selective banning can result in over-blocking, where legitimate websites or services may get unintentionally blocked, causing collateral damage. In order to reduce such over-blocking, TSPs/ISPs will have to carry out regular monitoring and audit of the block-list.

While there may be some technical solutions to mitigate some of these challenges, no solution is foolproof and will completely ensure the desired outcome. **Unless the internet is completely shut down in an area, it will always be possible for someone well-equipped with specific knowledge, to bypass the blockage and access the specific OTT services and websites that are purported to be blocked. Thus, selective banning from the TSP/ISP end would not serve any purpose.**

Considering the above, we suggest that the Government should consider source-level blocking, i.e., it should directly engage with the OTT service provider or website or hosting server /operator in question so that the desired outcome may be achieved without any significant difficulties – as elaborated further in the response to Q11 below.

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.

Airtel Response:

Yes.

There is a need to put in place a regulatory framework that is effectively implementable and one that involves the right stakeholders in the process. As suggested in the response to Q10, source-level blockingwould be much more effective than relying on TSPs/ISPs.

The TSPs/ISPs have no control over the systems of OTT services/websites and, hence, there will always be ways to work around the blocking if it is done through the TSPs/ISPs. Instead, if the OTT service/website purported to be blocked is directly involved in the process, it would be better equipped to devise a procedure for effective blocking as it would be better aware of how its systems work and how they can be controlled.

Even currently, when certain content is to be taken down because it violates any laws/ rules, the Government issues orders directly to various OTT service providers and websites on which the content is present. For instance, social media companies were ordered to take down 9849 links from their platforms in 2020.[10] Similarly, in the year 2023, until March 10, 974[11] social media URLs, accounts, channels, pages, apps, web pages, websites, etc under Section 69A of the Information Technology Act, 2000. The same approach needs to be adopted in cases of the selective blocking of OTT services and websites.

Accordingly, there is a need to put in place a regulatory framework for the selective banning of OTT services and websites. Since the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 are specific to the telecom sector, they would prove inadequate in case any of the OTT application services were to be blocked. Hence, the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 should be appropriately modified to include the OTT services and websites, in order to maintain uniformity.

While Airtel believes that selective banning of OTT services and websites is a desirable alternative, however, it has to be done at the source level. Direct involvement of the concerned OTT services and websites in the process will also ensure that the normal data continues to run without having any negative impact on the economy or other digital services.

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.

Airtel Response:

All OTT service providers are in possession of enormous amounts of data, and each one of them can give rise to cyber security and other threats. In order to avoid gaps in security measures, the regulatory framework should be equipped to deal with all kinds of OTT services.

[10] https://indianexpress.com/article/technology/social/content-blocking-orders-by-govt-and-courts-to-twitter-soars-48000-8021423/
[11] https://www.thehindu.com/news/national/4999-youtube-links-blocked-so-far-it-ministry/article66630488.ece

Therefore, all classes of OTT services, i.e., OTT communication services, OTT broadcasting services and OTT application services, should be covered under the regulatory framework for selective banning of OTT services in the country.

Also, please refer to the response to Q10 above. Various technical challenges arise when the selective/complete banning is carried out by the TSPs. Source-level blocking is much more effective. Therefore, the regulatory framework for selective banning should hold the specific OTT service providers – and not the TSPs – responsible for blocking.

It is also pertinent to highlight here that the systems for compliance with various security conditions under the license, like lawful interception and monitoring, have evolved over a long period of time through constant collaboration between TSPs and authorities.

Similarly, **the regulatory framework for blocking of OTT services and websites may be finalised in consultation with OTT service providers and websites as they are the appropriate source-level stakeholders.**

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.

Airtel Response:

There may be a need to selectively ban specific websites – apart from OTT services – to meet the purpose, depending on the circumstance.

As in the case of OTT services, all classes of websites should be included under the regulatory framework for selective/complete banning, in order to enable the Government to issue blocking orders to requisite websites as and when necessary.

That said, it is again re-iterated that **there are multiple technical challenges involved in selectively banning websites from a TSP's end. Therefore, the Authority should explore the option of source-level blocking and look at ways of involving the entities hosting the specific websites for effectively achieving the desired objective.**

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.

Airtel Response:

We have submitted our detailed comments in Preamble and in response to Q8 & Q9 on the requirement of sustainable investments in the networks, and the need for a fair share contribution. The topic being critical for sustainability of industry, the TRAI may even consider initiating a separate and detailed consultation on this issue to decide on modalities of fair share.