# Bharti Airtel Limited’s Response to TRAI pre-consultation paper on “Net Neutrality”

## The Vision of Digital India

The Government launched a flagship program named ‘Digital India’ last year with a vision to transform India into a digitally empowered society and knowledge economy.

As per the Government[1], **a well-connected nation is a prerequisite to a well-served nation.** Once the remotest of the Indian villagers are **digitally connected through broadband and high speed Internet,** the delivery of government services electronically, to every citizen, targeted social benefits and financial inclusion can be achieved in reality. **The emphasis is on providing high-speed Internet connectivity across the length and breadth of the country by deploying information and communications technology infrastructure, optical fibre, and last-mile connectivity options offered by wireless technologies in a manner that is affordable, reliable and competitive.**

## Where we stand.

The ambition to create ‘Digital India’ through affordable and reliable broadband-on-demand is laudable. However, we have a lot to do to make this vision successful. Today, India ranks[2] 131st in fixed broadband penetration and 155th in mobile broadband penetration despite being the 10th largest economy of the world in terms of GDP[3].

Thus, the Indian TSPs are required to make massive investments to aid for the achievement of the above vision. Today with around 331.66 million total Internet users[4], Internet penetration in India is very low. Of these, a mere 136.53 million users[5] have access to broadband. Therefore, ‘Digital India’ and ‘Broadband to All’ will require a significant expansion of TSPs’ networks and this expansion certainly rests upon the ability of TSPs to secure more investments, acquire more data spectrum and increase deployment of infrastructure/towers/optical fiber etc.

However, the financial health of the Industry is in dismal condition. The Industry is laden with net debt in excess of Rs.3.80 lac crores but still it faces demands of more than Rs.5 lac crores of investments to meet the vision of Digital India.  Indian telecom sector is subject to one of the highest taxes and levies in the world. It is making an ROCE of 1%

[1] http://www.digitalindia.gov.in/content/vision-and-vision-areas

[2] http://www.broadbandcommission.org/documents/reports/bb-annualreport2015.pdf

[3] http://www.thehindubusinessline.com/news/in-terms-of-gdp-indias-economy-is-10th-biggest-world-bank/article6196736.ece

[4] http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf

[5] http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf

which is an unsustainable situation. **So, without critical infrastructure and investment in place, there cannot be Internet access – neutral or otherwise.**

In addition, we need to create demand for Internet especially when the state of broadband is looking weak. To drive the next phase of Internet growth, we need to do more to expand the broadband penetration. A significant part of population is unaware of the benefits of being connected to Internet. TSPs and other relevant stakeholders need to come together to expand the reach of Internet across the country. They will need to eliminate entry barriers that prevent users from coming on to the ecosystem. It will be critical to offer content and use cases that encourage people to come online.

**Therefore, it is vital that the public policy on Net Neutrality should be directed towards achievement of development goals of the country by enabling 'affordable and quality broadband', 'massive network investments, 'universal Internet access', 'net equality', 'ease of doing business', 'promoting specialized services' 'innovative business models for promoting Internet access' and 'low entry barriers to Internet"**

A para wise, detailed response to the questions posed in the consultation paper is as under:

Q1.**What should be regarded as the core principles of net neutrality in the Indian context? What are the key issues that are required to be considered so that the principles of net neutrality are ensured?**

**Airtel's Response:**

1. We believe that India needs a **rational, proportionate, objective, ex-post policy** framework for Net Neutrality, which is directed towards achievement of developmental goals of the country without compromising the rights of Internet users. Any policy framework of net neutrality, which leads to lower investments and sub-optimal broadband infrastructure, will only weaken the vision of 'Digital India'.

2. The public policy of Net Neutrality should holistically enable the overall communication Industry including device Internet eco-system to meet the vision of 'Digital India' and 'National Telecom Policy'. Some of the core principles of Net Neutrality, which may be deliberated in the upcoming consultation paper are:
   - To provide seamless access to Internet from all kinds of devices and Access medium.
   - To promote network investments for universal broadband access
   - To bring more people online through various innovations

- To enhance the affordability of broadband access
- Ease of doing business
- No blocking of any content, applications, services and devices unless directed under the law
- No degradation or throttling of lawful Internet traffic based on content, applications, services and devices.
- To promote the synergies of network, content and application providers with light touch regulations and commercial freedom
- To implement 'Same Service, Same Rules' across all types of service providers
- To recognize an unbridled right of users to access lawful content of their choice without discrimination;
- Transparent Traffic Management Practices
- To promote Fair, Reasonable and Non-Discriminatory Business Practices
- To foster Specialized Services/Enterprises services with assured QoS and with commercial tie-ups

3. In addition to the above, the policy framework of net neutrality should not be limited to:
    - Wireless only since access to Internet should be agnostic to the type of bearer. For example, wifi offload of mobile networks is happening seamlessly, carrier aggregation using wifi and mobile is happening simultaneously.
    - TSPs only, but should include content/application providers and handset manufacturers and other stakeholders of Internet eco-system as well. For example, TSPs are regulated very heavily with respect to storage of location, call and SMS records while the same is freely accessible by any application which renders the exercise ineffective. Another example could be that barring or enabling access using device shortcuts may be construed as against the principle of net neutrality. Similarly, the customer privacy has now three significant vulnerabilities – device, network and content providers and any regulation limited to TSPs will not address the entire issue of data protection. Further, any pricing and tariff regulation on content in India should not be only applicable to TSPs but to the Internet companies who are pricing the content/applications who should also come within the ambit of same framework.

4. In fact, in its report, DoT committee has recognized that the public policy interventions need to ensure that **affordable access and investment in broadband**

**infrastructure are not counter-posed against the core principles of Net Neutrality.** We concur this and believe that any policy on Net Neutrality should promote **'net equality' and 'network investments'.**

5. Further, the Committee has recognized that the primary goals of public policy in the context of Net Neutrality should be directed towards achievement of developmental aims of the country by facilitating "Affordable Broadband", "Quality Broadband" & "Universal Broadband" for its citizens along with the following approaches:
   - **Expand access to broadband;**
   - Endeavour through Digital India to **bridge the digital divide, promote social inclusion**;
   - **Enable investment** , directly or indirectly, to facilitate broadband expansion;
   - Ensure the functioning of competitive markets in network, content and applications by prohibiting and preventing practices that distort competitive markets;
   - Recognize unbridled right of users to access lawful content of their choice without discrimination;
   - Support the **Investment-Innovation Virtuous Cycle** and development of applications relevant and customized for users.

6. In summary, we request TRAI to deliberate upon the above-mentioned core principles of Net Neutrality as well as its applicability on TSPs, website, content/application providers, and handset manufacturers, in the upcoming consultation paper.

Q2 **What are the reasonable traffic management practices that may need to be followed by TSPs while providing Internet access services and in what manner could these be misused? Are there any other current or potential practices in India that may give rise to concerns about net neutrality?**

Airtel's Response:

1. The Internet traffic is increasing globally and the increased demand is reinforcing the need for effective traffic management. It is estimated that by 2018, there will be nearly four billion global Internet users and around 80 per cent of all traffic will be video, which will require enormous network capacities to fulfill the increasing demand. TSPs would need adequate resources to effectively manage the traffic and efficiently meet this demand.

2. Due to the enormous volume of traffic currently being served by the wireless networks, effective traffic management will play a critical role due to the below mentioned reasons:

   a. **No guarantee that service levels of mobile networks will be the same at all locations.**

      Wireless network providers have to deal with several constraints to ensure satisfactory QoS to all subscribers. Some of these are highlighted as below:

      - **Distance from a cell-site:** A primary consideration when evaluating the reliability of a mobile connection is the distance between the user and the closest cell site. Moving away from a connecting cell tower degrades the connection and provides a somewhat variable quality of experience as a consumer moves from one site to another.
      - **Localized congestion:** Localized factors lead to traffic spikes that can potentially bring about congestion failure in wireless networks. Localized congestion may increase during festivals, occasions with large public gatherings, and at times of emergency.
      - **Time sensitive traffic:** The Internet akin to broadcast networks, displays off-peak and peak hour patterns of traffic. Internet traffic increases during peak hours and smart traffic management serve to ensure that peak hour activity doesn't cripple networks.
      - **Networking technology (2G/3G/4G):** QoS in wireless networks also varies according to the connecting technology. Assuring QoS becomes increasingly challenging as a consumer switches from one technology to another during periods of mobility.
      - **Devices:** The devices along with different operating systems use the network in different ways which creates different service experience for users.
      - **Applications:** The application design using the data service places an important role in the customer experience.

      Due to all the above mentioned factors coupled with and continuously increasing Internet traffic, the TSPs face challenging constraints that limit their ability to ensure a uniform level of quality of service for a wireless connection. In fact, the only way each bit of data has a uniform quality of service is when every user has the same device located at the same place;

all Cells have uniform distribution; network is not constrained because of the unavailability of the spectrum; all Cell sites function on the same technology and every user is equally distant from the Cell site.

**b. Traffic Management has always been part of wireless networks.**

- Today, Internet Protocol (IP) based networks have been designed to route IP data packets according to their performance characteristics. Packet delivery needs to take into account multiple characteristics – type of traffic, destination of packet, availability of routing options, network propagation environment, etc.
- For example, essential services like emergency services, remote diagnostics, etc. should be prioritised over delay-tolerant services such as messages, file sharing and emails to meet the consumer expectations of different services and to support critical communication needs.
- Traffic management was used even in previous generation of networks and the need today is much greater than ever before due to the wide variety of available services with different requirements. Similar to the prioritisation of voice calls in 2G and 3G networks, voice calls are also prioritised over 4G networks based on open standards developed by international standards organisations.[6] The sophistication of traffic management will evolve as an increasing number of complex applications began to use mobile networks and a growing number of device types access those applications.[7] Further network prioritization was always envisioned as part of the Internet Protocol and its implementation was consistent with the laid-out specifications.
- It should also be appreciated that traffic management takes place at every level of the Internet. Providers of hand sets, browsers, virtual market places and other services such as Google, Microsoft, Nokia and others use traffic management to improve the delivery of their pages on the Internet and to optimize third party content using the same methods as those used by ISPs. Optimization, caching, intelligent traffic management and providers of Content Delivery Networks have a business model based on obtaining revenues by improving quality of

[6] For example, 3rd Generation Partnership Project (3GPP) has standardised Voice over Long Term Evolution (VoLTE) for the provisioning of voice calls on LTE networks based on managed resource allocation for VoLTE calls.

[7] The vision for next generation 5G networks illustrates this complexity where billions of devices, from phones to cars, could communicate to each other within fraction of seconds.

experience for end users. Net Neutrality must address the complete value chain and result in holistic benefits to the end user and restrictions, if any, must apply equally to all players in the value chain.

- The efficient way to manage multiple types of traffic is not to treat all traffic with the same priority but to match the prioritisation of the network resources to traffic characteristics and service requirements.

c. **Benefits of traffic management**

Today, the Internet operates on best effort architecture and Telecom Service Providers use traffic management to minimize the incidence and impacts of congestion. This ensures that the maximum possible users get the best Internet experience. Traffic management is also necessary for technical, operational and commercial requirements such as:

a) **Management of Network Congestion:** This is especially required for mobile broadband networks where signal strength varies from location to location, in localized congestions, during mobility, and the non-availability of the spectrum at all locations. Traffic management helps in providing a better online experience for end users by using available network capacity more efficiently and helps network operators in supporting a larger number of concurrent users.

Traffic management techniques are critical for managing congestion in mobile networks, which are inherently capacity constrained. Traffic Management techniques provide an essential layer of efficiency which alongside ongoing investments in speed, capacity and coverage, also help network operators cope with the rapid growth in data traffic. Appropriate traffic management techniques can improve the efficiency of broadband networks by 25% to 35%, which not only results in better quality of service but also reduces costs for consumers in the same proportion.

b) **Network integrity:** Traffic management techniques help TSPs to protect end users from online threats such as spam and malware. Without such protection, end users would be exposed to a range of undesirable impacts ranging from lower network performance;

cluttered inboxes; greater risk of identity theft; to device infection with viruses.

c) **Child protection:** Traffic management also helps in applying content filters that limit access to age-appropriate content on the internet.

d) **Delivery requirements:** Traffic management help operators to ensure that delay-sensitive services such as voice calls and video streaming to keep working smoothly. This may require the use of prioritization techniques. Services that are non-real time, e.g., email, web browsing etc., can be provided at lower priority in periods of congestion with no impact on user experience.

e) **Emergency calls**: Routing calls to emergency services too can be more efficiently performed.

f) **Enterprise Customers:** Providing premium services for enterprise customers is required for their business needs. However, it should not lead to any compromise on the quality of service for ordinary users.

3. In fact, the DoT Committee has recommended that **legitimate traffic management practices may be allowed** but should be "tested" against the core principles of Net Neutrality. As per DoT's committee, general criteria against which these practices can be tested are as follows:
   a. TSPs/ISPs should make adequate disclosures to the users about their traffic management policies, tools and intervention practices to maintain transparency and allow users to make informed choices
   b. Unreasonable traffic management, exploitative or anti-competitive in nature may not be permitted.
   c. In general, for legitimate network management, application-agnostic control may be used. However, application-specific control within the "Internet traffic" class may not be permitted.
   d. Improper (Paid or otherwise) Prioritization may not be permitted
   e. Application-agnostic congestion control being a legitimate requirement cannot be considered to be against Net Neutrality. However, application-specific control within the "Internet traffic" class may be against the principles of Net Neutrality.
   f. Mechanism to minimize frivolous complaints will be desirable.

4. Globally, reasonable traffic management practices have been permitted to enable the TSPs to manage their network efficiently and optimally. Some examples are as under:
    a. In Singapore[8], ISPs and telecom network, operators must comply with IDA‟s information transparency requirement and disclose to end-users their network management practices.
    b. European Parliament in its regulation dated 25th November 2015 recognizes that the objective of reasonable traffic management is to contribute to the efficient use of network resources and optimization.
    c. The Body of European Regulators for Electronic Communications (BEREC) in guidelines on the implementation by national regulations of European Net Neutrality Rules (June 2016) recognizes the importance of implementing reasonable traffic management measures. As per BEREC, the regulators should assess whether the traffic management measures are:
        i. Transparent, non-discriminatory and proportionate
        ii. Objectively different technical QoS requirements of traffic categories
        iii. Not based upon commercial considerations.
        iv. Shall not monitor the specific content.
        v. Shall not be maintained longer than necessary.
        vi. Distinction from exception traffic management measures such as blocking, slowing down, alteration, restriction, interference with, degradation, and discrimination between specific content, applications or services or specific categories thereof.

5. **In light of the above, the issues related to traffic management may be deliberated in the upcoming consultation paper including the measures related to transparency.**
6. **Furthermore, ISPs are currently given a list of sites to block but various browsers that proxy traffic (UCWeb, Opera, Chrome with data saver on) bypass any such restrictions. In order to avoid such situations, which makes the government/court's direction of blocking the sites ineffective, TSPs could also add blocking of piracy sites as a legitimate use of site blocking or throttling as sophisticated practices, which otherwise have made URL level blocking ineffective.**

**Q3. What should be India's policy and/or regulatory approach in dealing with issues relating to net neutrality? Please comment with justifications.**

[8] https://www.ida.gov.sg/~/media/Files/PCDG/Consultations/20101111_Neteutrality/NetNeutralityExplanatoryMemo.pdf

**Airtel's comments:**

In continuation to our response to question no. 1 and 2, we further state that the policy framework of Net neutrality also requires deliberation on the following aspects:

## 1. Same Service, Same Rules:

a) TSPs concern revolves around OTT communication services (OCS), which are direct/close substitutes of the services offered by licensed TSPs. We believe that such OTT service providers must play by the same rules and regulations that the TSPs have subject to. This is central to the "Same Service, Same Rules" principle, which in no way violates the net neutrality principle. OTT communication service providers (OCSPs) must therefore, comply with the following:

- Ensure that national-security obligations and lawful interception requirements are met. Today calls made on VoIP (Voice over Internet Protocol) cannot be intercepted and servers who process these calls are outside the country. This is a grave national security risk.
- Requirements such as providing call records to law enforcement agencies should be complied with.
- It must contribute towards national development and rural infrastructure through payment into the USO fund the way telecom service providers do.
- It should contribute to all levies – similar to licensed voice service providers.
- Data privacy and customer protection rules be applied to them as is applicable to TSPs.

b) At present, there is a huge pricing arbitrage, of the order of 1:6, between VoIP (data services) and Voice Services. Differential charging for VoIP is required to eliminate the arbitrage which leads to subsidization of rich data customers using smart phones by the customers using voice through ordinary feature phone. VoIP/OTT Voice also creates a non-level playing field between licensed TSPs providing voice services and OTT Communication Service Providers providing same services. With the growth of smartphones and 3G/LTE network, OCSPs are carrying huge VoIP traffic over the data network of TSPs. For example, WhatsApp[9] carries more than 100 million VoIP calls every day.

c) The DoT committee has also recognized the importance and criticality of 'same service, same rules' between TSPs and OCSPs. As per committee, OTT domestic voice

[9] https://blog.whatsapp.com/10000625/WhatsApp-Calling-100-million-conversations-every-day

call services have the potential of significantly disrupting existing revenue models of TSPs. The committee further concluded that the existence of price and regulatory arbitrage between OTT voice and operator voice services requires a calibrated response to bring about a level playing field.

d) To promote the network investments and level playing field, the committee has recommended that domestic OTT communication services should be regulated through exercise of licensing powers available under Section 4 of the Indian Telegraph Act. However, the committee has asked the government to exclude OTT international voice communications, OTT chat and OTT messaging services from the licensing requirement on the same basis as that for OTT applications services.

e) We believe that the exclusion of OTT International voice communications, OTT chat, OTT messaging services require a reconsideration on the following reasons:

   a. Unlike OTT application service, voice and messaging services in India are the licensing activities exclusively permitted under Section 4 of the Indian Telegraph Act. Therefore, we believe that there is no justification to treat OTT voice communication/messaging services and PSTN voice communication/messaging services differently. The principle of regulatory similarity should be considered for all voice calls and messaging services. Therefore, all OTT communication services should be subjected to same licence and security conditions as being applied on TSPs in India.

   b. All OTT Communication Service Providers are offering messaging and voice communication services (both domestic and international) under a single application. Therefore creating a distinction between OTT messaging and OTT voice (as well as between domestic and international) is not possible under a single application. Therefore all OTT Communication services should be treated similarly.

**Therefore, any regulation on OTT communications and/or charging of underlying data services should follow the principle of "Same Service, Same Rules."**

## 2. <u>Specialized Services:</u>

a) In order to encourage innovation, any policy on net neutrality may consider permitting specialized services. However, such services are different from normal Internet access service and may drive additional private investment in the broadband network. As technology advances and turns concepts such as remote surgery, distance-learning, M2M, driverless cars and the Internet of Things into realities, the ability to offer specialized services could be critical in promoting consumer interests and national policy priorities. The provision of such services/content requires a specific level of quality and assured QoS. For example, M2M requires a creation of a differential quality network to meet the technical requirement of M2M/IOT. Therefore, the provision of specialized services will promote greater investments in broadband infrastructure, especially without restricting the growth or capacity available for broadband Internet access services.

b) It is be noted that MB based pricing cannot be the only way of charging. It is neither suitable for customers who struggle to understand usage nor is it an accurate estimation of the cost of production of data. For example, some megabytes are consumed in a single session vs others over several sessions, which is much more costly. Similarly, MB based pricing doesn't take into account amount of signaling, strength of upload signal, level of voice congestion, etc which all impact cost of production. Thus, a use-case based pricing is necessary both for consumer adoption and promote IoT and other use cases.

c) Furthermore, in the Internet, few contents/services are dominating other types of Internet traffic. For example, Netflix now accounts for nearly 37% of peak web traffic in North America; YouTube accounted for 15.6%, web browsing was 6%, Facebook was 2.7%, Amazon Instant Video was 2.0% and Hulu was 1.9%. Globally[10], IP video traffic will be 82 percent of all consumer Internet traffic by 2020, up from 70 percent in 2015. Thus, a detailed deliberation on the consumption of Video would be needed as over half the consumption is likely to be video and needs to be treated specially. Video in general can cause huge congestion increasing call drops while Live TV needs prioritization due to its ephemeral nature. Protocols like eMBMS manage this through some version of "broadcast" which again is an innovation that needs differential treatment of traffic and pricing. Similarly recent development on UDP protocols also will land up traffic differentially from video based TCP/IP. Therefore, all these innovations will require different treatment of traffic and pricing models and thus, should be deliberated in the upcoming consultation paper.

*d)* DoT in its committee has also recognized the importance of managed/enterprise/specialized services. As per committee, managed services, perceived as enterprise-related services, get the highest priority of QoS along with voice and video. *This may be allowed without affecting the minimum guaranteed QoS of*

[10] http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

*'Best Effort Public Internet". This committee is of the considered view that managed services are a necessary requirement for businesses and enterprises, and suitable exceptions may be made for treatment of such services in the Net Neutrality context.*

e) Other jurisdictions have also recognized the importance of such services. For example, as per the Net Neutrality Regulation of European Union (November 2015)[11], the specialized services have specifically been permitted. As per this regulation:

   1. Providers of electronic communications with the public including providers of internet access services and providers of content, applications and services **shall be free to offer services other than internet access services, which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality.**
   2. Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services **only if the network capacity is sufficient to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and shall not be to the detriment of the availability or general quality of internet access services for end-users.**

f) Subsequently, in its recent draft guidelines on Net Neutrality (June 2016), BEREC[12], has recognized that "***there is a demand on the part of providers of content, applications and services to be able to provide electronic communication services other than Internet access services, for which specific level of quality, that are not assured by Internet access services are necessary. .. National regulatory authorities should verify whether and to what extent such optimization is objectively necessary to ensure one or more specific and key features of the content, applications or services and to enable a corresponding quality assurance to be given to end-users, rather than simply granting general priority over comparable content, applications or services available via the Internet access service and thereby circumventing the provisions regarding traffic management measures applicable to the Internet access services***"

[11] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN

[12] http://berec.europa.eu/eng/document_register/subject_matter/berec/public_consultations/6075-draft-berec-guidelines-on-implementation-by-national-regulators-of-european-net-neutrality-rules

g) Similarly, FCC in its February 2015 order[13] on 'Open Internet' has also permitted specialized services.

**We believe that a "light touch" model that highlights core principles that TRAI holds yet gives flexibility for innovation and technology development could be to expand the regulatory filings that telcos do for price plans. Similar filings can be done for arrangements deemed sensitive for potential abuse such as prioritization or differential pricing or new technology use. In case these principles are violated, TRAI has existing mechanisms at their disposal to take action, resolve disputes, etc.**

**Thus, we request that the above issues should be deliberated in the upcoming consultation paper. Needless to say that the provision of such services should be provided with enough freedom to both parties (TSPs and providers of specialized services) to work together and co-invest in building the telecom infrastructure through different business models, including two-sided pricing options/business models/differential pricing.**

**3. <u>Zero rated platforms:</u>**

a) Globally, the enterprises for a long time have been trying to get more customers on-board by providing a convenient method to connect to them. Toll free mechanism has worked well to bring more and more people on board. Some of these examples are toll free voice, try and buy, free sampling, business paid postage etc. Similar free sampling mechanisms will play an important role in bringing more customers on board for data services. This has become more critical as the data growth is slowing down in India.

b) Regulators across the world have acknowledged the potential benefits of sponsored data. While mindful of possible anti-competitive concerns, they have chosen to review such arrangements on a case-by-case basis (FCC, 2015[14] and EU, 2015[15]). We firmly believe that sampling of the Internet and allowing free experience of sites is core to Internet adoption. Pricing innovations such as zero rated websites hold great socio-economic merit, and as such must be evaluated pragmatically.  However, TRAI can review all such schemes to ensure that the differential charging/zero ratings are provided in a non-discriminatory and transparent manner.

[13] https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

[14] FCC Open Internet Order, 2015 available at https://www.fcc.gov/document/fcc-releases-open-internet-order

[15] file:///C:/Users/b0000741/Downloads/6075-draft-berec-guidelines-on-implementation_0%20(1).pdf

**c)** Therefore, we believe that marketing interventions like these have happened and will continue to proliferate in the interests of customers across industries. TRAI should encourage such innovations provided these are non-discriminatory to the consumers. It is important to note that **in the case of zero rating, social welfare increases because benefits are directly passed on to consumers and not to commercial entities**. **Further, such platforms encourage more users to explore the Internet and eventually become regular data users.**

**Q4. What precautions must be taken with respect to the activities of TSPs and content providers to ensure that national security interests are preserved? Please comment with justification.**

**Airtel's comments:**

1. We strongly recommend that under the '**Same Service, Same Rules'**, OCSPs should meet the national-security requirements.

2. Today, OCSPs are able to offer calls across telecom networks in India using strong encryption and deploying switching servers located outside the country. Hence, they effectively prevent any lawful interception and/or monitoring of calls handled in their switching servers/network. These players are not sharing subscription details of customers and/or logs of communications. In fact, some OCSPs facilitate spoofing of CLI, which makes it difficult to identify or locate the actual caller. Further, since their switching servers are installed in foreign countries, OTT's communication traffic from these servers can be intercepted by those foreign governments, but not by the Indian government.

3. National security agencies and DoT have often voiced their interest in having Indian TSPs intercept and monitor the VoIP traffic offered by OSCPs. Since TSPs merely provide Internet, they are unable to intercept and monitor services, which are provided in a strong encrypted form and through switching servers which are not under their control. Besides national security concerns, Indian TSPs also continue to risk violations of their licensing conditions, specifically the condition that mandates them to provide lawful interception and monitoring of each type of service/product including Internet/Internet Internet/Internet telephony passing through their networks.

4. An illustrative list of the  security norms which are today applied on TSPs but not on OCSPs are as under:
   - **Telecom companies are to be registered in India:** Telecom services/licences can be provided / obtained only by the Companies registered in India so that they can be subject to Indian laws. *A majority of companies of OTT players are not registered in India and are beyond the scope of any Indian law.*
   - **Domestic traffic to stay within India:** As per clause no. 39.23(iii) of UL; domestic traffic shall not be hauled/routed to any place outside India. *On the contrary, OTT players route India's traffic (message / voice from one person to another person in India) outside India as they have not placed their servers in India.*
   - **Network to be set up within service area or country:** As per clause no. 4.5 of UL, the network related elements (Short message Service Centre/voice switching center/MSC/media gateway, etc.) should be located in a service area or anywhere in India, subject to the scope of applicable licence. *On the contrary, OTT players have set up their switching network outside India for provision of telecom services to customers located in India.*
   - **Lawful interception:** As per clause no. 8.1.1 of UL (ISP), lawful interception and monitoring systems are to be set up by Licensee for Internet traffic including Internet telephony traffic at their cost. *On the contrary, OTT players do not provide live lawful interception in unencrypted & readable format to Indian security agencies.*
   - **Usage of Higher Encryption Key:** As per clause no. 2.2(vii) of ISP licence, operators can use encryption key up to 40 bit key length. If encryption equipment higher than this limit is deployed, it requires prior written permission from DoT and deposit the decryption key. *Since OTT players have deployed encryption equipment much higher than this limit (Skype use 256 bit AES encryption) and do not share decryption key, Indian security agencies cannot intercept the communication of Indian citizens/person located in India for lawful purpose.*
   - **Access to subscriber database:** As per clause 39.19 of UASL, DoT will have an access to the subscriber database of the Licensee. Indian telcos follow subscriber verification guidelines. *On the contrary, OTT players do not provide traceable identity/access of their Indian customers to Indian security agencies.*
   - **Maintenance of CDR/IPDR:** As per clause 7.1 and 7.2 of UL (ISP), telecom companies are required to maintain CDR/IPDR for Internet including Internet telephony services for a minimum period of one year. Therefore, these companies have to maintain log-in/log-out details of all subscribers for services provided such as Internet access, e-mail, Internet telephony, etc for a year. *On the contrary, OTT players are not required to follow these rules.*

5. In its report, the DoT committee has rightly recognized the difficulties being faced by the law enforcement agencies to intercept the OTT Communication Services. It recognizes that OTT communication services use advanced encryption technologies that impedes law enforcement agencies in to intercept and monitor. Such application providers are also not amendable to national legal jurisdictions. This inability to intercept and monitor has the possibility of compromising with national security and law enforcement capabilities.

6. The report also recognize that some of the security related measures may be in the nature of ex ante obligations (lawful interception, security audit etc) whereas others would be in the nature of ex post enforcement (public order, prohibited content, protection of privacy, data protection) (para 14.7). Therefore, the DoT committee has rightly recognized in its report that the national security is paramount regardless of treatment of Net Neutrality and therefore, recommended inter-ministerial consultations to work out measures to enforce compliance of security related requirements from OTT Communication Service Providers.

**Since the security regulations applied on TSPs are already clear, the same can be applied for OTT Communication Service Providers immediately. Therefore, we request TRAI to deliberate the national security requirements in the context of OCSPs in greater details in the upcoming consultation paper over this issue.**

**Q5. What precautions must be taken with respect to the activities of TSPs and content providers to maintain customer privacy? Please comment with justification.**

**Airtel's comments:**

1. Currently, telecom users are using many applications or services that seek to access, collect and otherwise use personal information and private data about users, which may be held on a mobile handset or generated by their use of a mobile application or service at the time of installation of application or as a default setting.

2. Such data could be - name, address, credit card details, age, gender, city, country, family details, educational qualification, mobile phone number, email address, location data, IMEI, IP address, location data, website visits, product uses data, online behaviour, call logs, messages, address book, notes, access to camera, videos.

3. Since most of the data lies with the telecom operators also, , DoT has put many stringent provisions in all telecom licences related to consumer privacy, confidentiality of customer information and sharing/transfer of customer information.

4. The privacy of customers using mobile services of Indian telecom operators is fully protected by telecom-specific rules and regulations as well as under IT Act. However, OCSPs are not subject to any such rules even though they provide substitute services. For example, Indian telecom operators have explicitly been prohibited to send the personal data of their customers outside India whereas there is no such restriction on OCSPs. Furthermore, since the servers of almost all OCSPs reside outside India, the personal data of all Indian customers de-facto remains outside India only. While some may argue that all these content providers are governed or can be governed under the IT Act; however, due to lack of a regulatory body to oversee the compliance of IT Act (like DoT, TERM Cells and TRAI do for telecom licence) as well as the fact that most OCSPs operate outside India, there is hardly any control over the personal data of Indian customers.

5. Apart from the above, in order to curb the menace of Unsolicited Commercial Communications (UCC), TSPs follow TRAI regulations of UCC and National Do Not Call Registry (NDNC), currently TCCCPR. Stringent penalty provisions for violation of these regulations have been prescribed by TRAI. However, OCSPs' services are outside the scope of this regulation, and therefore, they are able to generate significant volume of spam and unsolicited communication without any adverse effects.

6. Similarly, OCSPs are not subject to customer-centric regulation, such as;
   a. Metering and billing audits
   b. Quality of service
   c. Consumer Protection
   d. Telecom Tariff Orders

7. The DoT committee also recognizes the concern over this issue. As per the committee, there is a need for a balance to be drawn to retain the country's ability to protect the privacy of its citizens and data protection without rendering it difficult for business operations. One possibility is to identify critical and important areas through public consultations where there may be a requirement to mandate local hosting or retaining enforcement capabilities in cases of breach.

8. As evident above, privacy elements currently highlight the wide disparity between requirements on telcos and other entities (search engines, social networks, device OEMs, commerce apps, etc). Neither extreme is desirable – any apps can pull out and read location, SMS and call history from phones, negating any privacy that government is asking TSPs to take a lot of effort to protect. Therefore, a uniform policy framework related to data protection, consumer privacy for all stakeholders in Internet domain is an urgent need.

**Thus, we request TRAI to deliberate on the above issues in the upcoming consultation paper so that the rules related to sharing of personal data, security, safety and privacy of communication and other customer-related aspects are equally applicable to all stakeholders. Further, TRAI should also deliberate, in details, on Quality of Services, Metering and Billing, transparency of tariffs, non-discriminatory nature of tariffs offered by OCSP etc, in the upcoming consultation paper.**

**Q6 What further issues should be considered for a comprehensive policy framework for defining the relationship between TSPs and OTT content providers?**

**Airtel's comments:**

*Commercial relationship between content providers and TSPs*

1. Indian telecom market has one of the lowest tariff in the world in-spite of complete forbearance of tariff on voice, which has led the market to drive the prices. In an intense competitive market where TSPs have invested thousands of crores for creating the broadband network and buying data spectrum, a rigid tariff framework will slow the data penetration to a great extent. At this stage, when the technologies, services and commercial models of the Internet ecosystem are evolving, the best way is to allow the market forces to work freely to meet customers' expectations.

2. Internet is typically a two-sided market and both stakeholders – content providers and TSPs should have the flexibility to offer commercial propositions to each other. In a market-driven economy, commercial freedom and engagement are critical for attracting investments, running a business and delivering a value proposition to end customers.

3. The freedom to explore various commercial arrangements, including two-sided business models with other content and application providers will encourage the development of innovative services and sustainable business models. Such arrangements can benefit consumers and businesses by aligning investment. For

example, direct peering immediately improves performance between a website and customers of a TSP. Similar applies for caching at a TSP location. This is commonplace and such performance improvements are desirable and help reduce costs. By its very nature, it is a commercial arrangement between TSP and OTT operator and hence, the same should be permitted without any regulatory intervention.

4. We believe that any regulatory intervention on commercial arrangement between TSPs and the content providers tantamount to curbing the flexibility of operators to carry their business and therefore, should be avoided. The commercial flexibility between TSPs and Value Added Service Providers, both for "on deck" and "off deck", has worked extremely well for the entire VAS ecosystem and consumers.

5. Other markets, such as the European Union and the United States of America, that has recently adopted 'Open Internet Rules,' have recognized the technical and commercial flexibility to TSPs by providing TSPs with the freedom to enter into commercial agreements with third parties and relying on competition law standards for ex-post scrutiny of such agreements.

*Commercial relationship between OTT Communication Service Providers and TSPs*

6. Currently, TSPs spend a substantial proportion of their revenues earned from Communication Services such as voice, on the development of network infrastructure, purchasing spectrum, building towers, laying fiber, etc. Whereas, in case of services provided by OCSP, TSPs only earn revenue for the usage of data network and the revenue from Communication Service is earned, controlled and retained by OCSPs, which thereby, reduces the capability of TSPs to invest in building the network infrastructure.

7. Therefore, as providers of the same services, OCSPs also need to have the same responsibility to develop the infrastructure. In this context, we believe that the appropriate structure would have the following characteristics:
    a. A **Network Usage Charge:** A charge that is paid by an OCSP to TSP. This will be paid to the TSP as the vast majority of infrastructure investment will still be built by TSP but utilized by OCSP.
    b. **The Network Usage Charge should be usage based**: The charge shall be based on level of usage, i.e., on per minute basis as this would incentivize the OTT to optimize their service from a network efficiency perspective.
    c. **Network usage charges not to have any linkage to retail tariffs** in any form.

**Or alternatively, TSPs should be allowed to charge their customers for the use of data services for the OTT Communication Services so that the TSPs can continue the investments in the networks without increasing the cost for data services.**

**This is due to this fact that VoIP calls of OTT Communication Service Providers is not just a "principle" concern but also a significant economic one. Voice revenue helps pay for spectrum, capex expansion, significant taxation revenue. Allowing arbitration (both regulatory and technological) will have a huge impact on the financial health of sector, allied digital services, loss of government revenue through service tax, SUF, LF, etc and finally a huge blow on the financial sector due to telco's inability to pay back their debt.**

8. Furthermore, TSP and OTT Communication provider's tie-ups should not be misconstrued as Interconnections. The most fundamental aspect of the interconnection is that it only happens at the peer level, e.g., "voice to voice" or "data to data". While OTT communication service providers are application providers offering voice, TSPs in their capacity as data/internet providers are providers of bearer services only. Therefore, any association between OCSPs and TSPs should not be termed as an interconnection. At best, OCSPs can buy/negotiate the bulk data capacity as bearer infrastructure for their VoIP/voice services from the TSPs. Therefore, OCSPs should not be termed as interconnecting partners even if they were to be licensed within the country. Similarly, any arrangement with application/content provider should not be construed as 'interconnection '.

***We request TRAI to deliberate the commercial relationship between TSPs and content providers or OCSPs on the above lines in the upcoming consultation paper.***

<u>To summarize:</u>

**We request TRAI to deliberate on the following points in the upcoming consultation paper on Net Neutrality:**

1. **Appropriate legal and regulatory framework of net neutrality for TSPs, content/application providers, website and handset manufacturers so that any regulation is applicable on the entire Internet ecosystem**
2. **Core principles of Net Neutrality consistent with the vision of Digital India and Broadband Highways**
3. **Same Service, Same Rules between OTT Communication Service Providers and TSPs in the context of regulatory framework, national security, contribution to**

**national exchequer in the form of regulatory levies and taxes, protection of consumer privacy, data protection, etc.**

4. **Policy framework for uptake of specialized services such as M2M, remote medical diagnosis, disaster management, driverless cars, etc. and its related aspects**
5. **Pricing/Tariff framework for TSPs, content/application providers**
6. **Traffic Management practices of all stakeholders such as TSPs, content providers (CDN)**
7. **Data protection laws for TSPs, content/application providers and handset manufacturers**
8. **Provision of internet services to Enterprises Customers.**
9. **Provision of innovative pricing models (subsidized data, differential pricing)**