KOAN

05 July, 2016, New Delhi

To,

1. **Shri R.S. Sharma**
   Chairman
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

2. **Shri A. Robert J. Ravi**
   Advisor (QoS)
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

Re: Response to Pre-Consultation Paper on Net Neutrality

Dear Sir,

The TRAI pre-consultation on Net Neutrality is a commendable step towards ensuring a free and open internet in India. With India overtaking the USA as the second largest internet user base in the world, the prospects of the country evolving to be a global innovation hub are bright. In order to ensure that India fosters the right environment to propel social as well as economic growth, ensuring a free and open internet is the first step. We are happy to contribute to the developing jurisprudence of network neutrality in India. In this regard, we are presenting our response to the pre-consultation paper on net neutrality.

Background

We welcome TRAI's efforts in providing an impetus to the net neutrality discourse and opening up the space for future regulations to stakeholders and the general public. We respond to the "Net Neutrality Pre Consultation" with the hope that any subsequent regulations will be forward-looking in scope. A desirable objective for future regulations is the untethering of opportunities offered by the internet for public benefit and to foster competition while minimizing network security risks. This is particularly important in light of emerging technologies and relevant jurisprudence from across the globe, as outlined hereunder.

Government-led initiatives such as BharatNet and the private sector drive for increasing mobile broadband penetration and quality of service are integral for realizing programmes such as 'Digital India', 'JAM' and 'Smart Cities' as well as to strengthen economic growth. However, the future impact of the internet's impact is not limited to government services and citizen welfare. Increasing broadband penetration, particularly fiber optic connectivity, becomes even more integral considering its cross-sectoral implications, its potential to transform the service industry and disrupt existing ways of

doing business. For example, OTT communications services are commonly viewed as competition for traditional telecommunications. However, the transformation of communications services from telecommunications to being network agnostic represents a step towards convergence. That is, separation of the application layer from the network layer provides an opportunity to enable emerging technologies such as the Next Generation Network (NGN)[1] wherein access technologies can be unified into future converged all-IP networks.

Similarly, while broadband demand and quality of service is currently driven by OTTs which consequently occupy large bandwidth such as the case of internet video traffic, bandwidth usage patterns are expected to be disrupted further with the emergence of the 'Internet of Things'.[2] It is expected that emerging and future technologies will "create new legal and policy challenges that didn't previously exist, and…amplify many challenges that already exist"[3]. Thus, although internet-based companies are considered to be competing with more traditional sectors such as broadcasting and retail, it is untenable to extend existing regulations to this dynamic, evolving sector.

While we can leave the potential regulatory dilemmas posed by such technologies unaddressed for now, any extant and future regulations should be cognizant of the dynamic nature of this sector. It is equally important to highlight that the existing regulatory vacuum has bolstered innovation by providing low barriers to entry. Further, important issues such as standardization has been stakeholder driven as exemplified by the Internet Engineering Task Force (IETF), an open international community. In short, we need dynamic regulations that may be readily altered and updated to match technological evolution.

The subsequent sections document our response to questions posed by the Telecom Regulatory Authority in the 'Pre Consultation Paper on Net Neutrality'.

Questions 1

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?

Response

Net neutrality propounds that every bit of information travelling over the internet should be treated equally irrespective of the user, source, destination, application, platform or content. It effectively means that one bit should not be prioritized over the other.

In recent years, net neutrality has become a matter of public policy consideration and many countries have either introduced or are considering reforms to preserve it. The

[1] See generally http://www.itu.int/osg/spu/ngn/index.phtml (ITU, 2003).
[2] See generally http://www.itu.int/en/ITU-T/techwatch/Pages/internetofthings.aspx (ITU).
[3] The Internet of Things: An Overview, Internet Society, October 2015, p. 34. Available at https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf

methods to address net neutrality differ, based on a variety of factors ranging from infrastructure, priority – access or speed, market forces etc.

A comparative analysis of relevant norms in force in various jurisdictions (Annexure 1) indicates that the following principles are the cornerstones of an effective net neutrality regime –

a. No blocking – ISPs may not block access to legal content, applications, services and non-harmful devices.

b. No throttling – ISPs may not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non-harmful devices.

c. No paid prioritization – ISPs may not favor some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind—in other words, no "fast lanes." This rule also bans ISPs from prioritizing content and services of their affiliates.

d. Enhanced Transparency – ISPs are required to disclose accurate information regarding the network management practices the ISP undertakes, speed, performance and commercial terms of their services which a user might need to make an informed choice.

While the abovementioned factors are found across jurisdictions, countries like USA and Brazil have extrapolated these principles to include additional safeguards, namely:

a. General Conduct rules – The U.S. Open Internet Rules 2015 include a catch-all 'general conduct rules'. These rules act as the last safety net to ensure that ISPs do not indulge in any activity which breaches the principles of open internet and might not have been covered under the other regulatory provisions.

b. Enhanced Privacy – Marco Civil da Internet, Brazil's extant internet regulatory legislation has pioneered in laying down the foundations of enhanced privacy. While protecting the overarching principles of privacy it provides for compensation in case of material or moral damage resulting from breach of privacy. It also provides for detailed provisions for ensuring confidentiality of data transmitted over the internet, its storage, use and disposal.

Japan and EU's regulation also contain implicit privacy protection provisions by deterring practices like deep packet inspection.

Apart from countries which have created a regulatory framework to ensure net neutrality, countries like Japan and Australia rely on market force interaction to ensure a free and open internet. Japan employs a co-regulatory approach – wherein ISPs come up with their own traffic management best practices while the telecom regulator (MIC) monitors the competitiveness of their practices; and Australia relies on anti-trust mechanism and strong consumer protection laws.

While laying down an effective framework for network neutrality in India, due care must be taken to ensure that international best practices are adapted to the Indian context. Despite being the second largest Internet market in the world, internet penetration in India is far less from global standards. With 332 million internet subscribers, about 72% of India's population still remains unconnected. Out of 332 million, about 60% subscribers access narrowband services (<512 Kbps). Thus the question before India is not only to increase access, but also to improve the quality of internet access. This can be achieved by improving network infrastructure while ensuring that internet access becomes affordable.

Globally, the scope of unfettered innovation offered by a free and open internet has driven the investment cycle thereby ensuring that while network infrastructure improves, the prices are regulated competitively. Thus, we require a framework that fosters healthy competition and ensures that innovation drives growth in the market.

In the Indian context, and based on impact of net neutrality regulations across various jurisdictions (Annexure 2) it is recommended that the following principles be considered as basic net neutrality norms –

- No blocking, throttling or improper prioritization.
- Enhanced transparency
- No unreasonable traffic management practices

These principles and related norms are detailed in responses to the following questions.

Question 2

What are the reasonable traffic management practices that may need to be followed by TSPs while providing Internet access service 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?

Response

Generally, any regulation of traffic management would first require understanding the operational effects of traffic management techniques employed by Indian internet service providers. BEREC (EU) and Ofcom (UK) have previously commissioned investigations into traffic management techniques and user experience.[4] It is recommended that an empirical investigation be commissioned, based on pre-determined criterion such as:

[4] See:
i. A view of traffic management and other practices resulting in restrictions to the open Internet in Europe, BEREC and European Commission. Available at https://ec.europa.eu/digital-single-market/en/news/view-traffic-management-and-other-practices-resulting-restrictions-open-internet-europe
ii. A Study of Traffic Management Detection Methods & Tools, By Predictable Network Solutions Ltd for Ofcom, UK, 2015. Available at http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2015/traffic-management-detection.pdf

- Available traffic management techniques.
- Traffic management practices widely employed by ISPs.
- Location of the traffic management application along the entire digital delivery chain.
- Appropriate measures, tools and methods for traffic management detection.
- Factors that impact quality of service and techniques for monitoring the same.
- Identify when traffic management techniques improve and degrade the average quality of service generally for internet access and specifically for individual applications.

Similarly, since the underlying principles of net neutrality depend on user choice and control, relevant investigations may be commissioned to determine the demand side of the internet ecosystem.[5]

Specifically, in light of the Report of the Department of Telecom Committee on Net Neutrality, it is recommended that the following specific observations be taken into account:

"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."

Transparency and adequate disclosures by TSPs to users and regulators is an integral aspect of net neutrality and should be observed across the board based on certain criteria as enumerated under the Response to Question 3.

"Unreasonable traffic management, which is exploitative or anticompetitive in nature, may not be permitted. Further, Improper (paid or otherwise) prioritization may not be permitted. 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."

Traffic management may be classified into the following categories, as considered in the DoT Committee Report, 2015:

1. Differentiation

Differentiation includes packet prioritization or de-prioritization of applications. Reasonable differentiation practices may be employed for optimizing services. Unreasonable practices would harm user choice and the 'virtuous cycle of innovation', as detailed in Annexure 3. Thus, it is recommended that reasonable and unreasonable traffic management practices may be demarcated based on the following considerations:

i. Reasonable differentiation - Generally, differentiation between applications may be considered reasonable when conducted for delay or time sensitive applications such as VoIP or video streaming. It is recommended that the following qualifications be taken into consideration in the interest of the consumer:

[5] See: Transparency in internet traffic management, By Kantar Media for Ofcom, UK, 2012. Available at http://stakeholders.ofcom.org.uk/binaries/research/broadband-research/1145655/traffic-kantar.pdf

- Suitable traffic management detection techniques may be deployed to investigate whether certain types of traffic (VoIP, P2P, video etc.) are being unreasonably throttled, prioritization based on type of customer (eg. retail over wholesale consumers) are subject to permanent restrictions, are managed for all users or certain users, are deployed during certain time-periods (peak work hours, post-work hours), differentiate between ingress (incoming traffic) and egress (outgoing traffic) etc.
- Such differentiation should not discriminate between the same type of traffic and may be qualified through quality of service regulations. While the general practice is to ensure that all services are delivered on best effort basis in cases of congestion or other reasonable differentiation, it is equally important to establish that a minimum quality of service be ensured.
- Such differentiation may be limited by ensuring robust expansion of the underlying infrastructure to match growing customer demand. Thus, in accordance with the TRAI Act and as stated in the Hon'ble Supreme Court's judgment in COAI v. TRAI, TRAI can ensure "that service providers provide the necessary funds for infrastructure development and deal with them so as to protect the interest of the consumer."[6]

  Pertinently, TRAI issued guidelines on contention ratio in 2009 to ensure quality of service through availability of minimum bandwidth to users. However, whether existing contention ratios have resolved bandwidth issues experienced by users requires monitoring.

ii. Unreasonable differentiation – Application specific differentiation may be considered as an example of unreasonable differentiation. The U.S. case of Netflix v. Comcast demonstrates the ability of ISPs to unreasonably throttle traffic from specific applications to leverage commercial considerations (please refer to our response to Question 2 for a detailed discussion on interconnection). While the basis of contracts between service providers tend to be tiered to reflect the underlying complexity of the network, blocking or throttling traffic from specific applications for commercial considerations is a clear violation of the underlying principles of net neutrality. Thus, it is recommended that such application specific throttling or blocking be considered unreasonable.

   It is further recommended that adequate mechanisms for stakeholders to report instances of existing unreasonable differentiation be established and such traffic management be monitored. Adequate complaints and auditing mechanism may be developed for future complaints of unreasonable traffic management as elaborated under Question No. 3.

2. Network Security and Integrity

[6] Para 40, Civil Appeal No. 5018 of 2016, Supreme Court of India.

Traffic management may be considered reasonable in cases of emergency, network congestion and to maintain network security and integrity.

3. Other factors

- Business considerations such as specialized services and data caps.

  Specialized services are closed electronic communication networks (CECN) offered as customized enterprises solutions that may be delivered over TCP/IP. Although, such services are considered as being outside the internet domain and net neutrality, CECNs may impact quality of service as observed in the case of the Norwegian TSP Telenor[7] and thus should be considered while monitoring traffic management. Thus, it is recommended that suitable qualifications be explicated for CECNs based on a no harm criterion (no detrimental impact on general internet services) and a need based criterion (need for customized optimization).[8]

  Similarly, data caps are employed as tools to limit congestion. However, existing data caps may be investigated vis-à-vis network capacity and user experience.

- Legal restrictions such as for illegal websites/ services, spam may be handled as per the procedure laid down under extant laws.

- Generally, any internet traffic management practices to singularly promote commercial interests may be considered unreasonable.

"Traffic management practices like DPI should not be used for unlawful access to the type and contents of an application in an IP packet. Traffic management is complex and specialized field and enough capacity building needs to be done before undertaking such an exercise. Mechanism to minimize frivolous complaints will be desirable."

It has emerged that multiple jurisdiction have prohibited deep packet inspection (DPI) for breaching privacy. Monitoring mechanisms to prevent unlawful access through DPI must be determined.

It is reiterated that, given the underlying complexity of network management, further expertise needs to be relied on to determine best practices. Generally, any consequent norms will have to undergo routine upgradation to resonate with innovations in technology and industry standards.

---

[7] In 2011, one of Norway's largest ISPs Telenor decided to charge high bandwidth consumers (eg. Youtube) and prioritize specialized services to ensure quality of service while limiting other data services on a best efforts basis.

[8] Similar criteria have been adopted in other jurisdictions such as the EU. Specifically, Article 3 (5) of Regulation (EU) 2015/2120 specifies –

"Providers of electronic communications to 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. 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."

Further, if any traffic management techniques are allowed beyond the reasonable practices described above, it is important to distinguish between fixed broadband and wireless broadband, as they represent different traffic capacities. Specifically, current network capacities for fixed broadband may be adequate and may not require traffic management.[9]

Question 3

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

Response

1. Generally, net neutrality norms should –

- Not hinder user control over what they access over the internet;
- Not discriminate between the same class of services;
- Should not be anti-competitive or be detrimental to innovation and small businesses/startups;
- Should not prohibit standard marketing practices such as limited promotional offers.

2. Along with the recommendations for network management, the following criteria may be considered –

- The primary rules for net neutrality i.e. no blocking, no throttling and no improper prioritization (paid or otherwise) may be enforced.

- Transparency is pivotal to ensure TSP accountability and user satisfaction. In this regard, the following three aspects are integral for a robust transparency framework:

  i. Self-declaration: Despite having its shortcomings, it is important for TSPs to declare their practices to their customers before the user enters into a contractual relationship with the TSP for its services; in order to make an informed choice. Existing self-declaration criteria and formats have been specified by TRAI for Quality of Service norms. It is recommended that TSPs also declare their compliance with net neutrality norms in their terms of services and on their websites. Further, compliance to self-declaration norms by ISPs should be monitored by TRAI.

  ii. Adequate disclosure mechanisms: It is expedient to lay down adequate disclosure norms for TSPs to communicate their practices to their users. Hitherto, users have experienced lower download speeds than what they have paid for. User

[9] In this regard the DoT Committee observed –
"*Also relevant to the issue is the nature of network development brought about by investment in infrastructure. Networks that rely more on optical fibre (fixed) than spectrum (mobile) are less impervious to network demands by user. Spectrum resource being inherently limited brings technological limitations on QoS for Internet delivery over mobile unlike optical fibre which has the capacity to expand to accommodate increased demands on its bandwidth resources*." (Para 2.6)

experience may also be affected by distance from towers, reasonable or unreasonable network management practices etc. In this regard, it is recommended that minimal disclosure norms for TSPs should extend to:

- Network management practices in general as well as specific notifications of those practices that are likely to impact the user's experience. Further, where network management practices are used for congestion control or as an emergency measure, TSPs should provide post-facto notifications of the same with reasonable evidence.
- Quality of service and performance including contention ratio, actual download speeds, data packet loss, data caps etc.

iii. Auditing on a case by case basis: It is recommended that the practice of auditing be implemented to determine complaints of net neutrality violations against TSPs on a case by case basis. Further, mechanisms to determine cases for auditing and monitor the process should be investigated such as establishing a co-regulatory body as outlined subsequently in this section.

3. Exceptions:

While net neutrality principles must be balanced with welfare and business considerations, any exceptions to the principles must be construed narrowly to avoid undermining the concept of net neutrality. It is recommended that any exception to net neutrality norms should be clearly defined and be forward looking in scope.

It is recommended that the following exceptions may be taken into consideration -

1. Enterprise/ managed services – It is recommended that enterprise and managed services should be exempted from net neutrality principles as they are specialized services governed by contractual arrangements subject to qualifications as detailed in our response to Question 2.
2. Positive discrimination/ government services – It is recommended that essential online government services be made available for free to all users. However, no discrimination be made between users as this is a basic principle of net neutrality.
3. Limited promotional offers – It is recommended that limited promotional offers and other marketing practices be allowed to ensure online-offline parity.
4. Unlawful websites – Websites that violate extant copyright laws may be blocked following the procedure established under extant laws.
5. Preserving network security and integrity – It is a globally accepted principle that traffic management and other techniques may be adopted for network security, however, the same must be reasonable and subject to transparency norms.
6. Emergency measures – Emergency measures may include network security or national security considerations. Relevant criteria or an inclusive list of possible emergency situations be identified to clarify this exception.

With regard to the question of treating VoIP services as an exception due to its impact on TSP revenues, it is submitted that this will be detrimental for net neutrality. With regard to the contention that TSPs have lost considerable revenue to VoIP services, it is widely argued that while TSPs may suffer revenue loss due to VoIP services, revenue from data may set-off any such revenue loss, particularly in India where internet penetration is mobile-driven and is expected to grow. Further, it is submitted that revenue or profit and loss cannot be taken into consideration while determining the validity of regulations as upheld recently by the Hon'ble Supreme Court in the case of COAI v. TRAI[10]. By extension, the same consideration may not be taken into consideration while formulating regulations.

4. Implementation mechanisms:

i. Licenses – While TRAI may exercise its powers under the TRAI Act and issue notifications on specific aspects of net neutrality, in order to avoid extensive litigation and questions of jurisdiction, it is recommended that TRAI include net neutrality requirements by way of amendments to ISP licenses.

ii. Other models for enforcement and dispute settlement –

While the judiciary retains its powers over scrutinizing violations of net neutrality principles, in order to expedite dispute resolution and ensure a seamless experience for users it is recommended that alternate models for enforcing norms and settling disputes be explored.

In this regard, other models implemented include co-regulatory bodies implemented in jurisdictions such as Japan and Norway, in the following manner:

- Norway

Norwegian guidelines for net neutrality were developed by a working group consisting of Internet service providers, content providers and consumer organisations under the leadership of Norwegian Post and Telecommunication Authority (NPT). The guidelines encompass principles requiring neutral internet access services from providers in the Norwegian market, with the exception of specific forms of reasonable traffic management. The working group that developed the guidelines has subsequently functioned as a reference group that meets once a year to discuss developments in the industry and whether the guidelines are functioning as intended. While the model worked well for a period of time, recently the stand-alone co-regulatory model came into question when a large Norwegian ISP, Telenor, exited the group. Subsequently, Norway has proposed amending the Electronic Communications Act to provide a legal framework to ensure net neutrality.

- Japan

[10] Para 40, Civil Appeal No. 5018 of 2016, Supreme Court of India

Japan's approach is characterized by lack of formal, specific rules and broad authority granted by law to the regulator – Minister of Internal Affairs and Communications (MIC). In 2006, MIC's Telecommunications Bureau created a working group to provide recommendations on net neutrality. The findings of the working group though non-binding, were adopted in the New Competition Promotion Program 2010 that laid down principles of net neutrality for Japan. As a part of the recommendations, a group of four communication industry associations with MIC as an observer developed guidelines on packet shaping which forms the core of Japan's net-neutrality regulations.

Further, the following overarching factors may be taken into consideration for resolving disputes, as adapted from the United States' General Conduct Rule –

i. impact on competition;
ii. impact on innovation;
iii. impact on free expression;
iv. impact on broadband deployment and investments;
v. whether the actions in question are specific to some applications and not others;
vi. whether they comply with industry best standards and practices; and
vii. whether they take place without the awareness of the end-user, the internet subscriber.

Question 4

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.

Response

It is recommended that while national security is of critical importance, it needs to be balanced with adequate network security norms without compromising either. For example, while high encryption standards may interfere with the Government's surveillance abilities, network security requires adequate encryption standards to resist cyber-attacks and other criminal activity on the internet.

Further, it is foreseeable that network security will increasingly become a matter of national security as recognized in the National Cyber Security Policy, 2013. In this regard, it is imperative to develop cybersecurity infrastructure and capacities.

However, since national and network security issues go beyond net neutrality concerns it is recommended that the matter be decided by way of an independent consultation or suitable legislation.

Question 5

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

Response

Hitherto, relevant privacy principles have been set forth by the Report of the Group of Experts on Privacy headed by Justice A.P. Shah in 2012. Further, a draft Privacy Law is being developed by the government through the Department of Personnel. In the absence of a comprehensive legislation on privacy, corporate data protection is governed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

It is important to ensure that relevant data protection techniques are followed to ensure customer privacy. For example, data should not be collected unreasonably by apps and such collection should be subject to the well-established collection limitation principle[11] based on the criterion of purpose.

Further, as recommended in the response to Question 3, investigations on network management techniques such as Deep Packet Inspection should also investigate impact of specific tools on privacy.

However, privacy is a broader issue that covers both government surveillance and corporate data protection based on similar principles. It is recommended that in the absence of a comprehensive legislation the existing Rules be suitably updated by way of a separate consultation process that considers the right to privacy holistically.

Question 6

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

Response

At the outset, it is recommended that OTT content providers should not be subject to licensing or separate regulatory frameworks since not only would this interfere with the virtuous cycle of innovation it would serve as an unreasonable barrier to entry. Currently, the relationship between TSPs and OTT content providers is subject to the contractual arrangement between them wherein extant laws on anti-trust, competition etc. become applicable. It is recommended that the existing practice based on contracts continue to determine the relationship between TSPs and OTT content providers.

Two issues are brought to your notice for consideration -

[11] Principle 3 of the A.P. Shah Report deals with Collection Limitation and states –
"*A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.*"

1. Interconnection

ISPs connect users accessing the internet through other providers by means of interconnection. While interconnection occurs at the network level and between service providers, it impacts the debates on net neutrality. Essentially, the goal of net neutrality is to preserve the neutral nature of the network wherein all end-points on the network are equally capable of exchanging content/applications/services with all other end-points. For this purpose, OTT service providers are another end-point in the network, just as any other end users. At the network level, the distinction between OTT providers and other end users is spurious as a neutral internet allows internet access to OTT providers in the same way as any other end user and allows any end user to become an OTT provider. Thus, if OTT content providers are treated differently from end users, by way of extra charges or other forms of differentiation, the basic principles of net neutrality are compromised.[12]

In the case individual applications or services require peering between their networks (eg. CDNs) and eyeball or terminating ISPs, the general practice has been to allow settlement free peering as such arrangements impose low costs on the service providers beyond the initial infrastructural costs. Generally, peering arrangements are preferred as they increase performance by eliminating intermediaries that may add latency. Further, settlement free peering keeps barriers to entry low and ensures maximum benefit for the consumer. Similarly, while interconnect costs with transit ISPs (transit costs) are generally higher than for peering, the price for transit has been observed to decrease over time with greater competition, market maturity and sophistication of transit networks. Thus, factors such as competition and network expansion also impact interconnection arrangements and keep costs low.

To reiterate, peering with terminating ISPs is preferred as it is cheaper and increases performance thereby benefiting both service providers and users. The ability of content providers to connect to terminating ISPs without encountering access tolls or other barriers is key to maintaining the open flow of information and content on the Internet. Nonetheless, if further arrangements are considered necessary for ensuring quality of service, such arrangements should be based on fair contractual agreements without

[12] To illustrate - TSPs are interconnected through a high speed network by means of routers at both ends. User 1 and the OTT both pay TSP 1 to access the internet. In some arrangements, OTTs may not pay TSPs, however, since user demand is driven by OTT providers, TSPs benefit from the presence of OTTs and are compensated through increased user demand. Similarly, User 2 pays TSP 2 for internet access. When User 2 wants to communicate with User 1 or the OTT the interconnection comes into play, wherein TSP 2 accesses the users of TSP 1 through interconnection governed by their contractual relationship. If User 2 is accessing the OTT service, TSP 2 provides access till the point of interconnection with TSP 1. Thereafter, TSP 1 connects User 2 with the OTT. Therefore, any revenue split is done on the basis of the contractual relationship between TSPs based on the work done by respective TSPs in connecting their respective users. Since TSP revenues are driven by user demand the contractual interconnection arrangement between TSPs is integral for a seamless experience. However, if TSP 2 is allowed to charge the OTT for connecting its users to it, the OTT pays twice (to TSP 1 and 2) for the same amount of work done. Since the work is split between the TSPs to connect their users, their revenues are tiered according to their contractual arrangement. Thus, TSP 2 should not charge the OTT for interconnecting its users to preserve the basic principles of net neutrality.

resorting to throttling or blocking of applications. The U.S. case of throttling of Netflix by ISPs exemplifies how net neutrality may be compromised for commercial considerations. [13] It is recommended that suitable norms be established to prevent the same from occurring in the Indian context and protect consumers.

Thus, it is recommended that to preserve the basic principles of net neutrality TSPs should not be permitted to treat OTTs differently from other users by way of prioritization or discrimination. Any interconnection arrangement between OTT providers and TSPs should be settlement free as far as possible or determined by a contractual relationship between them without violating the underlying principles of net neutrality as outlined in our response to Question 1.

2. Copyright and other laws

While copyright issues do not fall within TRAI's jurisdiction, it is important to specify that net neutrality principles are only applicable for legal websites, services etc. Thus, it is recommended that blocking unlawful websites be allowed following the procedure given under extant law such as through a court order, order of an inter-ministerial committee etc.

[13] In the American context market factors such as lack of competition impacted the ISPs decision to throttle Netflix and leverage a paid peering arrangement. While at present the same market conditions may not be reflected in the Indian context, a future-looking regulation should account for any possible monopolies that are likely to be created by ISP mergers.

KOAN

Annexure 1

Comparative Table of Net Neutrality Regulations

S.N.	COUNTRY	BASIC REGULATORY FRAMEWORK		ADDITIONAL REGULATIONS
		Network Management Principles	**Transparency**	
a.	**Cautious Observation**			
I.	**Australia**	● No specific rules on net neutrality. However, the government is actively monitoring the issue. ● Reliance is placed on ex post competition laws and strong consumer protection laws. ● The National Broadband Network aims to increase penetration and choice of a wide variety of ISPs.	● There is a strong emphasis providing accurate, transparent and relevant information to consumers in relation to service terms and conditions.	N/A
II.	**France** Proposed draft legislation on the 'digital republic'.	● There is no specific legislation on net neutrality. ● In 2010, ARCEP (Autorité de Régulation des Communications Electroniques et des Postes) published 10 recommendations on the freedom and quality of internet access, non-discrimination of traffic, supervision of traffic management, increased transparency, monitoring the data interconnection market, the role of content providers and for increasingly technology-neutral devices. ● These recommendations are currently followed by market stakeholders. ● A national legislation on net neutrality is being drafted and will incorporate BEREC recommendations.	N/A	N/A
III.	**United Kingdom**	• No specific regulation. Ofcom's 2011 statement on Net Neutrality describes that the UK framework recognizes benefits of both 'Best Effort' internet access and Managed Services and allows them to co-exist. • UK follows a self-regulatory approach. All major ISPs have signed the Broadband	• ISPs should provide sufficient information to the users to enable them to make right purchasing decisions. • Information provided to consumers should include at least the following elements:	

		Stakeholders Group's Open Internet Code of Practice.	➢ Average speed information that indicates the level of service consumers can expect to receive. ➢ Information about the impact of any traffic management that is used on specific types of services, such as reduced download speeds during peak times for P2P software. ➢ Information on any specific services that are blocked, resulting in consumers being unable to run the services and applications of their choice.	
b. **Tentative Refinement**				
I.	**Japan** Guidelines for Packet Shaping (Japan Internet Providers Association), 2010 and Significant Market Power Regulations implemented by MIC.	● Japan relies on a co-regulatory approach where private bodies agree on reasonable network management practices while the regulator – MIC ensures the competitive behavior of ISPs. ● Increased network traffic should be primarily dealt with investments to enhance network capacity. Packet shaping has to be considered an **'exceptional measure'.** ● Packet shaping should be targeted at network congestion, the existence of which should be substantiated by objective data. ● Packet shaping must be non-discriminatory and adequate. ● Proper packet shaping must satisfy "validity of means" criteria. For example – throttling a certain application that occupies excessive	● Packet shaping involves analysis of the content of the data packets. In order to not jeopardize secrecy of communication, ISPs must obtain "clear" and "individual" consent of users. ● Since the packet shaping of a certain ISP might influence the entire broadband ecosystem, ISPs must disclose their packet shaping information beforehand, targeted at all stakeholders, including interconnecting ISPs and mobile virtual network operators.	● The Significant Market Power regulations ensure that the internet market is competitive. ● The MIC has designated the local network of NTT East and NTT West, which collectively holds more than 90% of broadband capable access lines, as '**Category 1 Designated Telecommunications Facility**' and mandates upon them to prepare non-discriminatory interconnection tariff for service based competitors

		capacity is acceptable, but completely blocking it is excessive. ● Throttling the traffic of heavy users is acceptable as long as they can enjoy the same actual speed as an average user		who seek to use their infrastructure.
II.	**European Union** Regulation (EU) 2015/2120, November 25, 2015. To be implemented through guidelines issued to national regulators by the Body of European Regulators for Electronic Communications (BEREC).	● ISPs should treat all traffic equally, without discrimination, restriction or interference, independently of its sender or receiver content, application or service, or terminal equipment. ● End users should have the right to access and distribute information and content and to use and provide applications and services without discrimination. In exercise of this right, the users are free to agree with ISPs on tariffs for data volumes and speed. Such agreements and any commercial practice of ISPs should not limit the exercise of these rights. ● Reasonable traffic management measures should be transparent, non-discriminatory and proportionate. It should not be based on commercial considerations. ● Differentiation in traffic should be permitted only on the basis of objectively different technical quality of service requirements of specific categories of traffic. ● Any traffic management practice going beyond such reasonable measures by blocking, throttling, restricting etc. should be prohibited except for 3 exceptions – ➢ In compliance of national legislations including criminal laws. ➢ To protect integrity and security of the network ➢ Impending temporary or exceptional network congestion.	● ISPs should inform end-users in a clear manner how traffic management practices deployed might have an impact on the quality of internet access services, end user's privacy and protection of personal data, possible impact of other services to which they subscribe on the quality of access and speed which they are able to realistically deliver. ● ISPs should also inform consumers of available remedies in accordance with the national laws in the event of non-compliance of performance.	● There is implicit privacy protection under the regulation. The regulation clarifies that reasonable traffic management *does not require techniques which monitor the specific content of data traffic* transmitted via internet access service.

III.	**Canada** Telecom Regulatory Policy CRTC 2009-657, 2009	CRTC recognizes Internet Traffic Management Practices (IMTP) as a necessary tool to manage network congestion. The IMTP guidelines issued by CRTC lay down the following – • Network investment is the primary tool to deal with network congestions. • Where IMTPs are employed, they should be designed to address a particular need and nothing else. • IMTPs should not be unjustly discriminatory or unduly preferential. • Retail ISPs may continue employing IMTPs without prior Commission Approval. The practice may be reviewed by commission based on concerns arising primarily through complaints. • When an ISP employs more restrictive ITMPs for its wholesale services than for its retail services, it will require Commission approval to implement those practices. These practices must comply with the IMTP framework and must not have a significant and disproportionate impact on secondary ISPs.	• ISPs must be transparent about the network management practices they employ as users need this information to make informed decision about the services they use.	• ISPs are not allowed to degrade real-time or time-sensitive traffic e.g. VoIP or video conferencing without Commission's approval
IV.	**Norway –**	• The Norwegian Post and Telecommunications Authority in collaboration with various industry stakeholders has laid down net neutrality guidelines based on the following three principles – **1. Internet users are entitled to an internet connection with pre-defined capacity and quality –** ➢ Internet users are to be given sufficient information about the characteristics of their internet connection. ➢ If additional services are being provided by ISPs, the subscription terms must specify how the use of other services will affect internet access. **2. Internet users are entitled to an internet connection that enables them to –**		

		➢ Send and receive content of their choice. ➢ Use services and run applications of their choice. ➢ Connect hardware and use software of their choice which are not harmful for the network, **3. Users are entitled to an internet connection that is free from discrimination with regard to type, content, sender or receiver's address etc.** ➢ The principle does not preclude reasonable traffic management practices to block activities that harm the network, compliance with an order, maintaining QoS for specific services which require this, deal with network congestion and to prioritize traffic as per user's wishes.		
c. **Active Reforms**				
I.	**United States of America** Open Internet Order, 2015 of the Federal Communications Commission. Adopted on February 26, 2015	**3 Bright line rules –** ● No Blocking ● No Throttling ● No Paid Prioritization N.B. – The rules are only applicable to Broadband Internet Access Services (BIAS). BIAS does not include, enterprise services, VPNs, hosting or data storage services. The rules are also not applicable to inter-connection	**Enhanced Transparency Rules –** ● ISPs are required to publically disclose accurate information regarding network management practices, performance and commercial terms of the services. ● ISPs are also supposed to accurately disclose promotional rates, data caps and packet loss. Users should also be specifically notified if a network practice is likely to affect their services.	**General Conduct Rules –** ● A *catch-all* standard to deter ISPs from using techniques which are outside the ambit of the bright-line rules. ● ISPs shall not unreasonably interfere or disadvantage – ➢ End-user's ability to access lawful content on the internet ➢ Edge provider's ability to provide lawful content

				and services.
II.	**Brazil** Marco Civil da Internet, 2014	Marco Civil da Internet ensures network neutrality in following ways – ● **Article 3(IV)** declares net neutrality as an underlining principle of internet governance. ● **Article 9** puts the onus on 'agent in charge of transmission, switching and routing' (functional equivalent of ISPs) to treat all data packets equally. ● Content of data packets may not be blocked, monitored, filtered or analyzed.	**Article 9** states that in the event of traffic discrimination or degradation, ISPs must – ● Act in a fair, proportionate and transparent manner. ● Provide users, in advance, with descriptive information on its traffic management and mitigation practices, including network security measures. ● Provide services on non-discriminatory commercial terms and refrain from anti-competitive practices. ● **Article 7 (VI) –** Provides for clear and complete information in contracts with ISPs in terms of data security measures undertaken.	**Emphasis on Privacy –** Privacy is guaranteed under two provisions – ● **Article 7 –** It mandates a citizen's right to privacy, the protection of such privacy and compensation for material or moral damage from breach of such privacy. ● The Article also mandates confidentiality of communications made by internet, confidentiality of stored private communication, non-disclosure of personal data to third party. ● The contract between users and ISPs should have a distinct consent clause, which would facilitate express consent of the user to collection, use, storage and processing of data. ● It mandates ISPs and Internet Applications to delete all personal data of a consumer upon his request or at the end of agreement between the parties. ● **Article 11 –** Article 11 subjects all operations involving collection, storage or processing of

				personal data must comply with Brazilian laws, if any of those acts are occurring in Brazilian territory. ● It also extends the jurisdiction of Brazilian Law to foreign entities providing services to Brazilian citizens.
III	**Chile** **Law No. 20.453 amending the General Telecommunications Act (Law No. 18.168)**	Article 24H of the Act lays down that ISPs - ● May not arbitrarily block, interfere with, discriminate against, hinder or restrict the right of a user to access any legal, content, application or service. ● May take any measure for traffic management or network administration provided that such practices do not negatively affect fair competition. ● Shall respect device neutrality by not limiting the right to use the internet on any legal device that does not impair use of the net or the quality of service.	● ISPs shall publish information on their website regarding access characteristics, speed, quality, distinguishment between local and international linking, and service nature and warranties.	● **Parental Control-** ISPs shall offer parental control services for content that is against the law, ethics or morals, at user's expense. ● **Privacy and Virus Protection -** The ISPs shall endeavour to ensure privacy to its users and protect its users from virus attacks and ensure security on the network.
IV.	**Netherlands** Amendment to Telecommunications Act, 1998 (Telecommunicatiewet)	● Article 7.4a of the amended Telecommunications Act states that an ISP must not hinder or slow down an application or service over the internet, unless such a step is necessary - ❖ To minimize the effects of congestion, whereby equal types of traffic should be treated equally. ❖ To preserve the integrity and security of the network of the service provider or the end user. ❖ To restrict unsolicited communication to end user based on his consent.	● If the infarction on the security and integrity of the network is caused by the traffic coming from the end user, the ISPs, before blocking or throttling the user's traffic, must notify him about the same so as to provide the user an opportunity to terminate the infarction. ● If due to urgency, the user cannot be notified prior to blocking or throttling of his traffic, ISPs	

		❖ To execute the legislative order of a Court. ● Providers of internet access services do not make the price of the rates for internet access services dependent on the services and applications which are offered or used via these services.	should notify the user as soon as possible.	

Annexure 2 -

Impact of Net Neutrality Regulations

Generally, net neutrality regulations across the globe are at a nascent stage of development. However, countries like Chile and Netherlands pioneered net neutrality legislations which have consequently had a tangible impact on the internet market and have evolved jurisprudence over time. While Chile and Netherlands enacted net neutrality legislations in 2010 and 2011 respectively, Norway introduced guidelines prepared and adhered to by the ISPs under the regulator's supervision as per their co-regulatory model in 2009.

Another observable trend has been diversity of approach based on the underlying problem or 'mischief' these regulations address. The success of a legislation/regulation can be judged by its efficacy vis-à-vis the intent behind enacting them. For example, while expanding access has been a concern for Chile, it has not been an issue for Netherlands which falls among jurisdictions that have the highest internet penetration in the world. Hence, the analysis focusses on the concerned jurisdictions' specific objectives.

Under this section we have analyzed the impact of net neutrality in four jurisdictions – the U.S., Chile, Netherlands and Norway, as follows:

1. Chile –

Chile was the first country to enact a net neutrality legislation prohibiting blocking, throttling and prioritization including zero-rated plans and strengthening transparency.

One of the main concerns while the legislation was being debated was that introduction of net neutrality norms may stifle innovation and make internet access costlier[14]. However, analysis of World Bank's data for internet users per 100 people[15], indicate that there has been a spike in the number of internet users since 2010, the year when Chile adopted the net neutrality law. Specifically, between 2011 to 2014, the number of internet users per 100 people increased from 52.2 to 72.4 at a CAGR of 11.52 per cent whereas between 2006-2010 the corresponding increase was at a CAGR of 6.87 per cent. By the end of December 2015, the internet penetration in Chile reached 76 per cent[16] which was 60.5 per cent in 2012 (CAGR of 7.90 per cent).

The Chilean telecom regulator Subtel has indicated that net neutrality norms have fostered a competitive innovation environment[17]. Further, there has been a reported

---

[15] World Bank data on Internet Users per 100 people - http://data.worldbank.org/indicator/IT.NET.USER.P2

[16] http://www.telecompaper.com/news/chilean-internet-penetration-reaches-76-in-2015--1144850

[17] http://www.bnamericas.com/en/features/telecommunications/what-can-the-us-learn-from-chiles-net-neutrality-law1/

increase in the number of companies entering Chile's telecom market, which was limited to only 4 major players till 2009.

In 2014, Subtel ordered telecom companies to stop offering free access (zero-rated plans) to social media as such practices violates net neutrality. However, this was countered by Pedro Huichalaf, Under Secretary for Telecommunications who claimed that telecom companies can provide free internet till the time it is open to all services[18].

Subsequently, Subtel created an exception for Wikipedia Zero, thus allowing its services under a zero-rated agreement. Subtel allowed such zero-rating services considering the fact that Wikimedia is a non-profit organization which does not collect personal information of the user for advertising and that Wikipedia's intent to provide access to knowledge is in-line with Subtel's views[19]. The move has however been criticized on the ground that this action might create a slippery slope.

The Chilean model primarily is an example of how a strong net neutrality regime ensures fair competition, helps in expanding access while bringing the cost of internet access down. It also exemplifies how zero-rating can be implemented to address specific needs of a market while not contravening net neutrality per se.

2. Netherlands –

In 2011, Netherlands became the first European country to enact a net neutrality law. The Dutch Telecommunications Act was amended to include Article 7.4a which prohibited ISPs from blocking or throttling user access and charging extra for using internet based communication services. These net neutrality provisions occurred as a reaction to KPN's 2011 decision to make users pay extra for the use of third-party messaging applications over 3G.

In 2013, the Dutch Consumer Authority, the Dutch Competition Authority and the Post and Telecom Regulator (OPTA) were merged into a single entity – the Consumers and Market Authority (ACM). This new entity has been given the mandate to enforce the Dutch net neutrality provisions. Four major decisions mark the evolving jurisprudence of Dutch Net Neutrality, as discussed below:

- 'Sizz App'

The first service investigated by was the 'Sizz app' offered Vodafone and Dutch media company RTL which zero-rated content it hosted. ACM ruled that putting this service outside the data plans of users was not in accordance with net neutrality legislation, pursuant to which Vodafone adjusted the offerings under the plan[20].

- Blocked services on free railway Wi-Fi

[18] https://panampost.com/belen-marty/2014/06/03/chile-to-fine-phone-companies-offering-free-access-to-social-networks/

[19] https://www.publicknowledge.org/assets/uploads/blog/Final_Paper-Jul_28-TM.pdf

[20] 2013, ACM Annual Report. Available at - https://jaarverslag.acm.nl/sites/default/files/2013%20ACM%20Annual%20Report.pdf

ACM also investigated internet access on trains of Dutch railway company NS which was offering free internet access to the on board passengers in collaboration with T-Mobile. The said service had blocked high bandwidth services like YouTube and Spotify. The practice was found to be justified as the network capacity on the free Wi-Fi network was limited and use of high-bandwidth apps would have caused congestion[21].

- KPN and Wi-Fi Hotspots -

KPN offered internet access through Wi-Fi hotspots at public places like airports. Through these hotspots users could access "Free Basic Internet" services. Services like BitTorrent, VoIP, FTP were excluded and in order to access them, the user had to either pay for a premium service or be a KPN customer. A company offering VoIP services reported this to ACM as a case of violation of net neutrality principles. In contrast to the railway Wi-Fi case, ACM found the practice as discriminatory and levied a fine of 2,50,000 Euros on KPN[22].

- Vodafone and HBO -

Vodafone allowed its customers free access to the HBO Go app for a period of three months with its 4G subscription. The app allowed the users to watch programmes aired on HBO cable and satellite television network. The offer was found to violate net neutrality as it steered users to a certain type of service which hampered freedom of choice and innovation. Vodafone was fined to the tune of 2,00,000 Euros[23].

The Dutch government recently voted to ban zero-rated services across Netherlands and is considering whether Internet should be classified as a public utility service[24]. The implementation of the net neutrality principles by Netherlands highlights the efficacy of legislative reforms and how they should be strictly implemented.

3. Norway –

Norway adopted the co-regulatory approach to ensure a free and open internet in 2009. Norwegian guidelines for net neutrality were developed by a working group consisting of Internet service providers, content providers and consumer organizations, under the leadership of Norwegian Post and Telecommunication Authority (NPT). The guidelines that were launched in 2009 encompass principles that require neutral Internet access services from providers in the Norwegian market, with the exception of specific forms of reasonable traffic management. The working group that developed the guidelines has

[21] Ibid

[22] ACM Decisions, 27.01.2015. Available at - https://www.acm.nl/en/publications/publication/14311/Fine-on-KPN-for-violation-of-net-neutrality-rules/

[23] ACM Decisions, 27.01.2015. Available at - https://www.acm.nl/en/publications/publication/14310/Fine-on-Vodafone-for-violation-of-net-neutrality-rules/

[24] http://arstechnica.co.uk/tech-policy/2016/05/net-neutrality-zero-rated-services-nixed-dutch-gov/

subsequently functioned as a reference group that meets once a year to discuss developments in the industry and whether the guidelines are functioning as intended.

Generally, the co-regulatory model worked well for Norway as the reference group did not felt a need to upgrade the guidelines[25]. In 2014, the NPT advised the ISPs to avoid zero-rating as it violated the principles of net neutrality[26]. However, in 2011, Telenor, one of Norway's biggest ISPs opted out of the voluntary net-neutrality code and expressed its willingness to charge data intensive services like YouTube as they consume too much bandwidth and thus they need to compensate ISPs. Telenor has also said that the paid up content will get quality of service guarantees while other consumers will be offered services on a best efforts basis[27].

Telenor voluntarily signed the net neutrality code in 2009. Such a volte-face brings out the demerits of a co-regulatory model and emphasizes the need for concomitant mandatory guidelines backed by appropriate sanctions. Significantly, in February 2016, Norway proposed amending the Electronic Communications Act to provide a legal framework to ensure net neutrality.

4. United States of America –

The United States of America adopted net neutrality regulations in 2015 following a series of litigation over the issue. The first attempt to ensure a neutral internet was made in 2004 when FCC laid down guidelines for preserving internet freedom which included four internet freedoms, encompassing net neutrality. In 2007, subscribers of Comcast noticed that the traffic on BitTorrent was being slowed down. Later it was discovered that Comcast and Cox Communications were throttling BitTorrent traffic at all times. In 2008, FCC ordered Comcast to stop interference with peer-to-peer traffic on its network. In 2010, the US Court of Appeals overturned FCC's anti-throttling ruling against Comcast observing that the FCC lacked "any statutorily mandated responsibility" to enforce network neutrality rules.

In December 2010, FCC approved the first Open Internet Order, which laid down the bright line rules and transparency clauses. The regulations were challenged by Verizon in September 2011 for falling outside FCC jurisdiction. In 2014, the Court upheld Verizon's claim and struck down the Open Internet Order on the ground of the lack of jurisdiction since broadband was an information service.

To rectify this, in the 2015 Open Internet Order, the FCC re-classified internet as a common carrier under Title-II of the Communications Act, 1934. While the FCCs ruling continues to be a matter of controversy, it has expanded its jurisdiction to implement net neutrality rules. Recently, the US Federal Court of Appeals upheld the validity of the Open Internet Order, 2015.

In the interim, another debate was initiated in the US regarding the cost of inter-connection. In 2014, Netflix, a major video on demand service which has more than 30

[25] http://eng.nkom.no/technical/internet/net-neutrality/the-norwegian-model
[26] https://gigaom.com/2014/11/18/pro-net-neutrality-norway-advises-carriers-to-avoid-zero-rating/
[27] http://news.heartland.org/newspaper-article/norway-isp-ends-net-neutrality-support; http://arstechnica.com/tech-policy/2011/01/a-nordic-change-of-heart-on-net-neutrality/

million subscribers in the US complained that ISPs were throttling its traffic. Eventually, Netflix entered into an agreement with Comcast and paid them an inter-connection fee to let its user's to get adequate quality of service. Interconnection since then has been a contentious issue. The Open Internet Order does not specify any interconnection mandate and provides for deciding disputes and violations on a case-by-case basis.

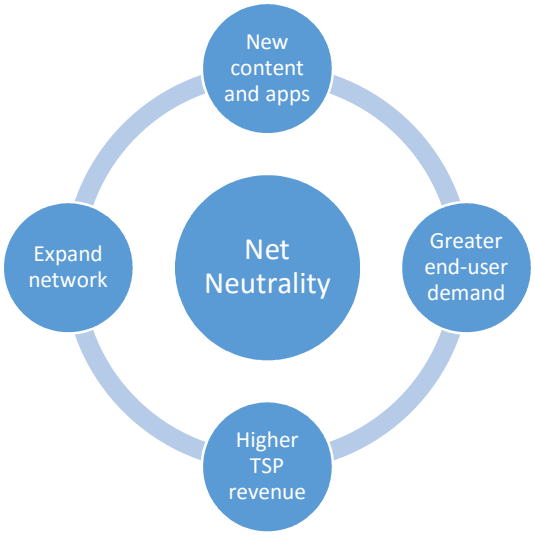
Annexure 3

The Virtuous Cycle of Innovation

First iterated by the FCC in its 2010 Open Internet Order, the virtuous circle of innovation was upheld in the case of Verizon v. FCC (2014) and US Telecom Association v. FCC (2016). It entails:

> *"The Internet's openness is critical to these outcomes, because it enables a virtuous circle of innovation in which new uses of the network—including new content, applications, services, and devices—lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses. Novel, improved, or lower-cost offerings introduced by content, application, service, and device providers spur end-user demand and encourage broadband providers to expand their networks and invest in new broadband technologies. Streaming video and e-commerce applications, for instance, have led to major network improvements such as fiber to the premises, VDSL, and DOCSIS 3.0. These network improvements generate new opportunities for edge providers, spurring them to innovate further. Each round of innovation increases the value of the Internet for broadband providers, edge providers, online businesses, and consumers. Continued operation of this virtuous circle, however, depends upon low barriers to innovation and entry by edge providers, which drive end-user demand. Restricting edge providers' ability to reach end users, and limiting end users' ability to choose which edge providers to patronize, would reduce the rate of innovation at the edge and, in turn, the likely rate of improvements to network infrastructure."*
>
> (FCC Open Internet Order, 2015)

The virtuous circle of innovation relies on a neutral internet for fostering innovation, as visualized below –



Essentially, innovations in OTT services generate user demand which leads to higher data revenues for TSPs and further improvements and expansion of network. Thus, although user demand for some kinds of OTT services may lead to congestion, shaping traffic of those OTT services which drive demand and innovation interferes unreasonably with the virtuous cycle of innovation and flies at face of the goal of net neutrality.

Alternate mechanisms of managing quality and offloading traffic are being leveraged at the network layer such as through interconnection. Further, OTT content providers rely on solutions such as Content Distribution Networks (CDN) to optimize performance, driven by market demand.

In this regard, the DoT Committee observed –

> *"Therefore, it is natural to assume that reasonable traffic management practices may need to be adopted by the TSP in order to ensure that unreasonable demands on network resources are not placed by a few real-time OTT applications to the detriment of all other traffic."*
>
> (Paragraph 8.4, DoT Committee Report)

It is humbly submitted that such an assumption will lead to an erroneous conclusion and impact net neutrality. Higher demand on network resources by some OTT providers is a natural consequence of user preferences. Any traffic management or other restrictions placed on the very OTTs that drive user demand will unreasonably interfere with the virtuous cycle of innovation.