

Date: 11 April, 2017

To,  
Shri Asit Kadayan  
Advisor (QoS)  
TRAI  
Tel. No. +91-11-23230404  
Email: advqos@traigov.in

**Subject: Comments by Novi Digital Entertainment Private Limited**

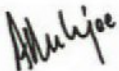
**Reference: Consultation Paper on Net Neutrality dated 4 January, 2017**

Dear Sir,

At the outset we are thankful to TRAI for involving all stakeholders in this consultation process. We appreciate TRAI's comprehensive consultation paper on this issue delving into the nuances of network neutrality. Network neutrality is important to unleash the immense potential of India's growing internet economy and TRAI's efforts in this direction are truly commendable.

We request you to take our comments on issues raised in the consultation paper embodied in this document on record.

Yours faithfully,  
For Novi Digital Entertainment Private Limited



Amrita Mukherjee  
Vice President - Legal

**Q.1 What could be the principles for ensuring nondiscriminatory access to content on the Internet, in the Indian context? [See Chapter 4]**

It is important to ensure that India's digital economy thrives within a conducive framework driven by free market forces, which has enabled the current state of innovation and growth. Given that the digital ecosystem is still at a very nascent stage, free market forces should continue to propel and shape its future. However, a free market framework also provides incentives to telecommunication service providers and internet service providers ("TSPs/ISPs") to engage in practices that are harmful to the open nature of the Internet and hamper the virtuous cycle of innovation. Therefore, not only is it in the interests of edge providers, but also users of the Internet, to have certain brightline rules set out to ensure that TSPs/ISPs do not indulge in anti-competitive and discriminatory behaviour. In the absence of any rules to protect the openness of the internet, TSPs/ISPs can act as gatekeepers and exercise an overwhelming capability to determine winners and losers on the Internet. Accordingly, a net neutrality framework should be made applicable to TSPs/ISPs and should comprise of the following principles–

- **No blocking:** The edge users of the Internet have a right to be able to access all end-points of the Internet, and this includes any and all content, applications and services that may be available. To this end, the Authority should consider adopting a broad and general no-blocking rule that prohibits TSPs/ISPs from blocking access to any lawful traffic transmitted between edge users of the Internet. This includes a prohibition on blocking any specific or class of content, application or service that an edge service provider may make available to other edge users of the Internet. The only exception to this rule should be reasonable traffic management (discussed in detail in response to Question 4(a) below).
- **No throttling:** Apart from prohibiting outright blocking, the Telecom Regulatory Authority of India (referred to as "Authority" for the purpose of this submission, and responsible for monitoring and supervision of the NN framework in India, as discussed in detail in response to Question 10 below) should also adopt a rule against preventing delivery of certain specific or class of content, application or services by 'throttling', slowing down access to or otherwise interfering with, degrading or impairing users' access to any lawful content, application or service. In the absence of such a rule, the no-blocking rule would be rendered ineffective because TSPs/ISPs may engage in conduct that

discourages access to certain content, application or services but does not technically amount to outright blocking them. The only exception to this rule should be reasonable traffic management (discussed in detail in response to Question 4(a) below).

- No paid prioritisation: Paid prioritisation result in dividing the Internet into a “fast lane” for edge services providers that are willing to pay TSPs/ISPs, and a “slow lane” for the rest. Prioritising certain content, application or services will automatically lead to degradation (such as lower bandwidth, high latency, etc.) of other content that is not the subject of such prioritization. This has the effect of creating artificial barriers for newer edge providers, impacting consumers’ choices, harming competition, damaging the open Internet and discouraging innovation. In the absence of a rule prohibiting paid prioritization, TSPs/ISPs will become gatekeepers of the nature and quality of content, applications and services accessible over the Internet and encourage them to prioritise their own services over other edge providers. Accordingly, the Authority should adopt a rule to prohibit TSPs/ISPs from speeding up or otherwise prioritising traffic (on the basis of type, origin or destination of content, or the means of its transmission) in return for any consideration.
- Transparency and public disclosure: Transparency and public disclosure of information with respect to traffic management practices, performance and pricing (including data caps and allowances) is essential to ensure principles of net neutrality and reasonable traffic management are adhered to. The Authority should require TSPs/ISPs to make timely and prominent disclosures and openly publish accurate information, accessible to edge users and edge service providers about any practice that could affect quality of service, subscriber charges, or otherwise affect subscriber experience. The disclosures should also include technical details such as the service technology, expected and actual access speed and latency, suitability of services for real time applications, the impact of specialized services and how they may affect the last mile capacity, etc. Please refer to response to Questions 8 and 9 below for additional details on disclosure requirements.

**Q.2 How should “Internet traffic” and “providers of Internet services” be understood in the NN context? [See Chapter 3]**

“Internet traffic” should be understood the way it is used in general parlance, i.e. to mean any and all data packets carried by providers of Internet services over their networks.

It is essential to properly define the term “providers of Internet services” to appropriately determine the scope and applicability of a net neutrality framework. Care has to be taken to ensure that the term is defined in a way that does not exclude various kinds of Internet services that are provided, such as:

- (a) Internet services provided over any technology platform such as wire, wireless, satellite, future projects such as Project Loon<sup>1</sup>; or
- (b) Providers of Internet services that either lease or own the infrastructure used to provide the services; or
- (c) Internet services provided for free, or for a charge, or even Internet data provided to users by third party TSP-agnostic platforms as incentives for undertaking certain actions; or
- (d) Internet services provided by private companies or public/government undertakings as part of a public Wi-Fi scheme; or
- (e) Internet services masquerading as “specialized services”; or
- (f) Services that are functional equivalents of Internet services or services that provide access to the Internet but are deployed in a manner to evade the net neutrality framework.

The EU and FCC have already defined Internet services in the manner provided below. The Authority could take a cue from the existing definitions to consider its own definition of “providers of Internet services”.

*EU – ‘internet access service’ means a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.*

---

<sup>1</sup> A project by Google to deliver Internet to remote areas through wireless routers hooked to balloons floating in the stratosphere.

*FCC - A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part.*

**(a) Should certain types of specialised services, enterprise solutions, Internet of Things, etc be excluded from its scope? How should such terms be defined?**

Specialised services – There are certain services that provide connectivity but require specific levels of quality that need to be maintained, which cannot be provided over the Internet. These services need to be optimized for the delivery of certain content, applications or services such as Voice over Internet Protocol (VoIP), Virtual Private Networks (VPNs), real time health services (for example, remote surgery).

Such services may be excluded from the net neutrality framework because they do not provide access to all or substantially all end-points of the Internet and they also require a certain standard of quality of service to be maintained to function optimally. Besides, such services are operated and maintained to perform certain very specific functions for particular applications and are not meant to provide general connectivity to the Internet.

However, care should be taken that any such “specialized services” should be narrowly and carefully defined to ensure services that provide a general access to the Internet or are functionally equivalent to an Internet access service are not exempt from the net neutrality framework under the garb of “specialized services”. Any “specialized service” should meet the following criteria:

- The optimization required for the service should be objectively necessary to meet the requirements for specific levels of quality. The service should be able to demonstrate that the specific level of quality required cannot objectively be assured over the Internet, and this should not be done merely by prioritizing specific content over comparable content.

- The service should not be used to reach large parts of the Internet. The service should not be usable to provide general access to the Internet or as a replacement to Internet access service.
- The service should not be a generic platform but rather a dedicated service meant to achieve a certain very specific function.
- The service should use some form of network management to logically isolate the capacity from that used by services providing a general access to the Internet, and should not limit, curtail or deteriorate the quality of or capacity available for the Internet access service.

The governing authority for any net neutrality framework should keep itself open for a case-by-case analysis of any such specialized services to determine whether they are being operated in a manner to evade the net neutrality framework. Accordingly, strict penalties should be imposed if it is found that Internet access services are masquerading as “specialized services”, or if such specialized services are not meeting any of the criteria mentioned above, or if such services are undermining investment, innovation, competition, and end-user benefits. Particular care should be taken to ensure that edge service providers over the Internet are not harmed in their ability to compete effectively merely because of the existence of a “specialized service” effectively and functionally performing the same function.

Internet of Things – The Internet of Things (“IoT”) is a fairly new concept and it should not be excluded from the purview of net neutrality. It is too early to assess the overall impact of IoT and the range of functions it can perform. It is a fast-developing technology with a variety of use-cases. Its applications range from everyday utility applications like smart home devices to public utility and governance applications like smart cities (e.g., traffic light system).

IoT is poised to grow to an installed base of 30.7 billion devices globally by 2020.<sup>2</sup> In India especially, IoT stands to play a significant role in government initiatives like smart cities and ‘Digital

---

<sup>2</sup> Roundup Of Internet Of Things Forecasts And Market Estimates, 2016, *available at* <http://www.forbes.com/sites/louiscolumnbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#22837ace4ba5>

India'. Further, IoT has been shown to be susceptible to hacking on numerous occasions, often leading to serious consequences. Even from a cyber-security perspective, IoT should be treated at par with the general Internet. Since we are still at a nascent stage of IoT development, a blanket exemption to IoT from the net neutrality framework may have unforeseen consequences. In the absence of net neutrality, IoT providers will be left at the mercy of TSPs/ISPs picking winners and losers, and true world changing innovation in this field will be lost at the altar of unfair competition and discriminatory practices.

**(b) How should services provided by content delivery networks and direct interconnection arrangements be treated? Please provide reasons.**

Content delivery networks (CDNs) and direct interconnection arrangements should not be subject to net neutrality. They form part of the backbone of the Internet infrastructure and do not connect to the last mile access network. Besides, CDNs and direct interconnection arrangements do not connect to all the end-points of the Internet and are the subject of private arrangements between contracting parties.

Even the DoT Committee Report on Net Neutrality 2015 is of the view that *“CDN is an arrangement for management of content as a business strategy. Making available one provider’s CDN to others on commercial terms is a normal business activity. Discrimination in access or adoption of anti-competitive practices by them is best left to be covered under the law related to unfair trade practices.”*

The FCC and EU have also excluded CDNs and direct interconnection arrangements from the scope of net neutrality and are adopting a wait-and-watch approach. Further, private arrangements for sharing content are the subject matter of exclusive rights granted to content owners by the Copyright Act, 1957 and should be left out of the purview of any net neutrality framework.

**Q.3 In the Indian context, which of the following regulatory approaches would be preferable: [See Chapter 3]**

- (a) Defining what constitutes reasonable TMPs (the broad approach), or**
- (b) Identifying a negative list of non-reasonable TMPs (the narrow approach).**

**Please provide reasons.**

Networks are evolving rapidly with new technological developments. Consequently, newer ways of optimizing and managing networks are also emerging. The day is not far when networks may be operated and managed purely by “artificial intelligence” that teaches itself how to best optimize a network. Given the fact that the current pace of development will lead to more and more novel ways of managing networks, it would be difficult to identify and list the various ways in which traffic over a network may be managed. Besides, various traffic, congestion or technical issues may arise that may require a response customized to each such unique scenario. What may be considered a reasonable traffic management technique may not be considered reasonable in a different situation. Also, a “negative list” of non-reasonable TMPs is not future-proof and will not take into account novel and innovative ways of managing traffic that may emerge as a response to each unique problem.

Whereas, on the other hand, laying down principles that guide behaviour by defining what constitutes reasonable traffic management practices (the broad approach) would be more beneficial for the following reasons:

- They merely guide behaviour to achieve a desirable outcome and do not foreclose options that may be available to a network manager to achieve the same result.
- Any such principles would be service, technology and circumstance agnostic. This will ensure that any future developments are adequately addressed by the principles and will ensure TSPs/ISPs are unable to get away with detrimental traffic management practices.



**Q.4 If a broad regulatory approach, as suggested in Q3, is to be followed: [See Chapter 3]**

**(a) What should be regarded as reasonable TMPs and how should different categories of traffic be objectively defined from a technical point of view for this purpose?**

Net neutrality is essential to preserve the open nature of the Internet and the virtuous cycle of innovation attributed to its openness. At the same time, it is essential to preserve the underlying architecture and backbone of the Internet – the networks themselves. Networks may get congested during peak hours, may be susceptible to security breaches, may be subject to denial of service attacks, or may need to be managed during emergencies to prioritise certain kinds of data over others. Therefore, to meet certain limited objectives, TSPs/ISPs should be allowed to undertake traffic management practices (“TMPs”) in specified instances only.

However, it is necessary to ensure that TSPs/ISPs do not misuse TMPs in a way that violates the net neutrality framework and does not interfere with the access, affordability and quality of services. To this end, it is important to lay down principles that TSPs/ISPs must follow while implementing any TMPs. Taking a cue from the global approach to traffic management, only such TMPs that conform to the following principles should be considered reasonable:

- Technical Objective Without Commercial Consideration: TMPs should be undertaken only to achieve certain technical objectives. No discrimination or differentiation should be practiced through TMPs for commercial consideration. So long as such practices are targeted towards certain base line principles like security, stability, congestion management, technical maintenance and law enforcement, and do not in any way or manner result in commercial gains to the TSP/ISP or is actuated for commercial consideration – the same may be justified.
- Non-Discriminatory: TMPs employed by TSPs/ISPs should not result in either application-specific or category based discrimination. As discussed in the response to Question 4(b) below, both application-specific and category-based discrimination will result in harms. As noted by TRAI in the consultation paper, the Internet operates on a first come first serve best efforts basis. This foundational principle of the Internet should be preserved and no discrimination should be allowed. Both application-

specific and category-based discrimination should be viewed equally strictly. Even the FCC Open Internet Order of 2015 emphasises this and states that “*network management practices that alleviate congestion without regard to the source, destination, content, application, or service are also more likely to be considered reasonable*”.<sup>3</sup> The only exception to non-discriminatory TMPs should be in case of actual emergencies (as discussed in response to Question 6(a) below) to prioritise certain content and communication over the network.

- **Proportionate:** TMPs employed by the TSPs/ISPs must be:
  - Necessary;
  - Proportionate;
  - Most suitable to achieve a certain objective;
  - Not manifestly inappropriate for the stated purpose; and
  - Maintained no longer than necessary.

The TSPs/ISPs should also be able to demonstrate that there was no other less-interfering yet equally effective alternative of achieving the same objective.

- **Preserving security and integrity of the network:** Certain exceptional TMPs may be required to preserve the security and integrity of the network. Such TMPs could include blocking of traffic from the offending IP addresses in order to prevent attacks. However, such TMPs should be implemented only on the basis of actual concrete security threats and not merely on the basis of a remote possibility of a threat. Since “security” is a very broad concept, the governing authority should carefully evaluate the justification provided by the TSPs/ISPs and impose harsh penalties in case of attempts to circumvent the net neutrality framework.

**(b) Should application-specific discrimination within a category of traffic be viewed more strictly than discrimination between categories?**

Neither application-specific discrimination nor category-based discrimination should be allowed in any case. Both of these forms of discrimination distort competition, stifle innovation, harm

---

<sup>3</sup> At para 220.

users and edge service providers, and will defeat the very purpose of setting up a net neutrality framework on the basis of principles as specified in the response to Question 1 above.

Video content is an important category of Internet traffic. In 2015, it accounted for 70% of the global Internet traffic, and it is expected to rise rapidly to account for 82% of the global Internet traffic by 2020.<sup>4</sup> Allowing for category-based discrimination would affect a huge chunk of global Internet traffic. Moreover, category-based discrimination should also not be allowed for the following reasons (as suggested by Barbara van Schewick in her submission to TRAI):

- TSPs/ISPs may favour certain categories of applications over others, thereby distorting competition.
- TSPs/ISPs may choose to deliberately discriminate against certain categories of applications to favour their own services. For example, TSPs/ISPs may discriminate against Internet telephony services to the advantage of their own telephony offerings.
- In the case of encrypted traffic, the TSPs/ISPs will not be able to identify the kind of traffic that it is carrying (such as email, financial transactions, etc.) and may end up throttling all encrypted traffic as a precaution.
- A TSP's/ISP's categorization of some kind of content may not necessarily be agreeable by edge users or edge service providers. The only way to challenge the categorization would be to complain to the governing authority, which would then require it investigate the categorization. This will only lead to higher costs of governing the net neutrality framework, not only for the governing authority but also for the edge service provider/edge user who may not be able to afford proceedings before the authority.

**(c) How should preferential treatment of particular content, activated by a user's choice and without any arrangement between a TSP and content provider, be treated?**

Preferential treatment of particular content activated by users' choice should be allowed subject to the following (as suggested by Barbara van Schewick in her submission to TRAI):

---

<sup>4</sup> Cisco Visual Networking Index: Forecast and Methodology, 2015-2020, *available at* <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf>

- the different classes of service should be available equally to all content, applications or services, and classes thereof;
- the user should be able to choose whether, when, and for which content, applications or services to use which class of service; and
- the TSPs/ISPs should be allowed to charge only its own customers for the use of the different classes of service.

Additionally, as has been done in the case of commercial calls and messages for consumers, a mechanism for transparency should be put in place that allows disclosure of customer choices and tracking the activation of such preferential treatment by TSPs/ISPs. TSPs/ISPs should be mandated to maintain a separate record of all customers that exercise this choice.

**Q.5 If a narrow approach, as suggested in Q3, is to be followed what should be regarded as non-reasonable TMPs? [See Chapter 3]**

Not applicable in light of response to Questions 3 and 4 above.

**Q.6 Should the following be treated as exceptions to any regulation on TMPs? Please elaborate. [See Chapter 3]**

All four of the following could be treated as exceptions to the principles of TMPs:

**(a) Emergency situations and services; -**

Emergency situations and services could be treated as exceptions. However, it is important to properly define and list such situations and services to limit the scope of the exception and its interpretation. For example, even the Unified License, which governs telecom service providers, explicitly lays down what constitutes emergency services, i.e. relevant public, police, fire, ambulance, coast guard or any other services so declared by the DoT.

**(b) Restrictions on unlawful content; -**

This could be considered a legitimate exception to the no-blocking principle. But any sort of restriction/blocking should only be applicable after an order from the court, except in cases of copyright infringement for which a takedown notice from the copyright owner should suffice.

**(c) Maintaining security and integrity of the network; -**

This is a reasonable exception subject to certain additional safeguards to ensure transparency and fairness. Please refer to responses to Questions 4(a), 8 and 9.

**(d) Services that may be notified in public interest by the Government/ Authority, based on certain criteria; or –**

Services notified in public interest by the Government/ Authority should not be considered an exception unless there is a clearly defined specific policy that provides guidance to the government on what can constitute ‘public interest’ in the context of reasonable TMPs. Carving it out as a blanket exception without any guidance will leave a broad power in the hands of the Government/ Authority to notify any service as being exempt from the principles of TMPs. Such an exception is very wide and a case could be made for several services/applications to be carved out from principles of traffic management. This could hamper innovation or have a significant impact on the open Internet. If at all, a very specific objective criterion should be laid down for any service to qualify for the government to grant it an exemption. The Authority should clarify what such “certain criteria” could be.

**(e) Any other services. –**

No other services should be exempted.

**Q.7 How should the following practices be defined and what are the tests, thresholds and technical tools that can be adopted to detect their deployment: [See Chapter 4]**

**(a) Blocking;**

**(b) Throttling (for example, how can it be established that a particular application is being throttled?); and**

**(c) Preferential treatment (for example, how can it be established that preferential treatment is being provided to a particular application?).**

Taking a cue from global practices (USA and EU), it would be best not to define the terms, but leave the terms to broader interpretation. This will allow the interpretation of the terms to be agnostic to technological advancement. Defining the terms could limit the applicability to certain

practices/parameters only. An open and subjective interpretation on a case by case basis allows for greater flexibility to aggrieved service providers to determine what they consider as reduced QoS for their users.

Currently, no technical tools are available for service providers to have a definite determination of whether their service is being blocked or throttled. The only information received is through user feedback or through performance metric analytics received from third party service providers. The only way to detect any blocking, throttling or preferential treatment is to connect the dots using the anecdotal data and arrive at a reasonable conclusion that a net neutrality violation may be taking place. Anecdotal data can be derived from network diagnostic tools such as the ones provided by MLab (to analyse the timing, trend, patterns, and recurrence to figure out if there is a violation of reasonable traffic management), user feedback, complaints from the service provider themselves, reports from third parties such as Akamai. On a prima facie conclusion that a violation may be taking place, the governing authority can undertake a detailed investigation using TSPs/ISPs logs, and inspecting the logs of the packets of data originating from a particular source, etc. If a TSPs/ISPs is found in violation of the NN framework on the basis of a reasonable conclusion, it can be penalized accordingly.

Currently, TSPs/ISPs are under no obligation to reveal any network management practices or technical/commercial reasons for unreasonable network management practices. Adequate measures should be put into place that allows service providers to raise QoS-related concerns with TSPs/ISPs through the governing authority and receive redressal.

**Q.8 Which of the following models of transparency would be preferred in the Indian context: [See Chapter 5]**

- (a) Disclosures provided directly by a TSP to its consumers;**
- (b) Disclosures to the regulator;**
- (c) Disclosures to the general public; or**
- (d) A combination of the above.**

**Please provide reasons. What should be the mode, trigger and frequency to publish such information?**

All three above (options a,b,c) will ensure adequate transparency. TSPs/ISPs should be required to publicly disclose accurate information regarding the TMPs, performance, and commercial terms (including data allowances and caps) of their service. TSPs/ISPs should make adequate disclosures that allow edge users to make an informed choice about the TSP's/ISP's services. Sufficient disclosures also enable edge service providers to develop and maintain their services.

True and correct disclosures also ensure that edge users and the governing authority are informed about a TSP's/ISP's traffic management practices, service performance, and commercial terms. Having a framework for transparency and accurate disclosures will act as a disincentive for TSPs/ISPs from misleading or deceiving edge users with claims about their service that are not consistent with the TSP's/ISP's disclosures to the governing authority. The disclosures should also be prominent, easily accessible and in plain language understandable by edge users, edge service providers and the governing authority.

Apart from making true and correct disclosures, the TSPs/ISPs should also be required to maintain the accuracy of such disclosures in a timely and prominent manner. TSPs/ISPs should be required to update their disclosures as soon as there is a material change in commercial terms, traffic management practices, performance characteristics, or any other part of the disclosures.

Disclosures should also be made on a quarterly basis in the form of filings to the governing authority and on the website of the respective TSPs/ISPs for edge users. Any anticipated instances of network management should be disclosed to consumers beforehand. Unanticipated instances of network management should be duly documented and disclosed immediately to the regulator. Such reports should disclose the justification for and the measures taken to manage the network.

The report should adequately demonstrate that the TSP/ISP has met the requisite criteria for implementing reasonable TMPs (as specified in response to Question 4(a) above).

**Q.9 Please provide comments or suggestions on the Information Disclosure Template at Table 5.1? Should this vary for each category of stakeholders identified above? Please provide reasons for any suggested changes. [See Chapter 5]**

Comments/Suggestions on some requirements in the disclosure template are provided below:

<i>Parameter</i>	<i>Disclosure Template</i>	<i>Comments/Suggestions</i>
<b>Application Specific Traffic Management</b>		
Are any services, content, applications or products always blocked on this plan?	Specify Yes/ No, list out Services, content, applications if applicable	The TSP should also be required to provide reasons for blocking such applications and if necessary permissions (if required) are obtained for such blocking.
Are any services, content, applications or products always prioritized on this plan?	Specify Yes/ No, list out Services, content, applications if applicable	The Service Providers should be required to provide the reasons for prioritizing certain content on a respective plan. Particularly, if the prioritization is mandated by a government order, etc. Links to such government orders should also be provided
<b>Application Agnostic Traffic Management</b>		
Are TMPs deployed during peak hours?	Specify Yes/ No	The impact of the TMPs deployed should also be explained.



What type of traffic is managed during peak hours?	-	The Service Providers should be required to confirm if they give preference to certain specific traffic during peak hours and why.
--	---	--

**Q.10 What would be the most effective legal/policy instrument for implementing a NN framework in India? [See Chapter 6]**

From the options that TRAI has suggested in the paper, the most suitable and appropriate would be for the government to amend the licenses governing TSPs/ISPs to incorporate principles of net neutrality, traffic management and transparency. In addition, TRAI could also issue QoS regulations to implement the framework. This will ensure light-handed regulation to implement net neutrality.

**(a) Which body should be responsible for monitoring and supervision?**

As per Section 11(1)(b)(i) of the Telecom Regulatory Authority of India Act, 1997 (“TRAI Act”), the Authority is the body responsible for ensuring compliance with the terms and conditions of the license. Accordingly, TRAI should be the governing authority responsible for monitoring and supervision of the net neutrality framework in India mentioned in the licenses as suggested by us in response to Q. 10

**(b) What actions should such body be empowered to take in case of any detected violation?**

Penalties should be proposed for breach of the license conditions in the form of fines, license review/suspension/revocation. Section 13 of the TRAI Act empowers TRAI to issue any directions to discharge its functions.

**(c) If the Authority opts for QoS regulation on this subject, what should be the scope of such regulations?**

In addition to amending the license conditions, TRAI could also issue QoS regulations incorporating the NN framework, including transparency and disclosure requirements for TSPs/ISPs, grievance redressal mechanisms, consequences for breach of the NN framework, conditions and restrictions for operating specialized services, and principles of reasonable traffic management that TSPs/ISPs have to adhere to.

**Q.11 What could be the challenges in monitoring for violations of any NN framework? Please comment on the following or any other suggested mechanisms that may be used for such monitoring: [See Chapter 6]**

**(a) Disclosures and information from TSPs;**

**(b) Collection of information from users (complaints, user-experience apps, surveys, questionnaires); or**

**(c) Collection of information from third parties and public domain (research studies, news articles, consumer advocacy reports).**

Challenges: Detection and demonstration of any violation could be the primary challenge in the efficient monitoring of the network neutrality framework. At the moment, the regulator, edge users and edge service providers lack the appropriate legal, and possibly technical, avenues to have potential violations addressed. For instance, a regular user of the Internet will find it difficult to assess whether a website is slowed due to ordinary heavy traffic or purposely by the TSPs/ISPs in violation of the network neutrality framework. Furthermore, based on a mere suspicion, the customer, edge service provider or the governing authority may not be able to take necessary actions due to the lack of adequate evidence at hand. Furthermore, TSPs/ISPs may make fraudulent, inadequate or misleading disclosures.

Suggested Mechanism: In addition to the response to Question 7 above –

- **Audit:** The governing authority should create a mechanism to enable edge service providers to periodically audit TSPs/ISPs through their respective industry associations by engaging independent technical auditors.

- **Grievance Redressal Forum for edge users:** The governing authority should provide for a complaint registration forum for the edge users to file their complaints (with the governing authority) based on any speculations of a violation of the net neutrality framework. Based on such complaints, the governing authority should monitor any such violations by the TSPs/ISPs and take necessary measures to rectify the violation. The TSPs/ISPs should also be required to provide for a complaint registration forum where its customers can file their complaints/ queries. The TSPs/ISPs should be required to provide responses to such complaints with adequate reasoning within a specific timeframe.
- **Grievance Redressal Forum for Content Providers:** The governing authority should also provide for a separate grievance redressal forum for edge service providers to file their complaints against TSPs/ISPs for any alleged violation of the net neutrality framework.

**Q.12 Can we consider adopting a collaborative mechanism, with representation from TSPs, content providers, consumer groups and other stakeholders, for managing the operational aspects of any NN framework? [See Chapter 6]**

The governing authority for the net neutrality framework should be responsible for monitoring and managing the operational aspects of the framework, This entity could be none other than TRAI. No multi-stakeholder model should be put in place.

**(a) What should be its design and functions?**

Not applicable in light of the response above.

**(b) What role should the Authority play in its functioning?**

Not applicable in light of the response above.

**Q.13 What mechanisms could be deployed so that the NN policy/regulatory framework may be updated on account of evolution of technology and use cases? [See Chapter 6]**

The net neutrality framework should be technology agnostic and this can be achieved by laying down broad bright-line principles for net neutrality, traffic management and transparency in the

license conditions of TSPs/ISPs. This will go a long way in ensuring that any technological evolution would be adequately covered under the framework. The governing authority should be responsible for continuously monitoring the market, undertaking periodic review of the market conditions, and assessing the relevance of the net neutrality framework to the evolution of technology and use cases.

**Q.14 The quality of Internet experienced by a user may also be impacted by factors such as the type of device, browser, operating system being used. How should these aspects be considered in the NN context? Please explain with reasons. [See Chapter 4]**

TSPs/ISPs should not be able to discriminate on the basis of the device, browser, or operating system used by the edge user. Any device, browser or operating system that is not harmful to the network should be permitted to connect to the Internet. Accordingly, any net neutrality framework should ensure that access provided to the Internet by TSPs/ISPs is independent of the kind of device, browser or operating system that the edge user employs.

The net neutrality debate concerns the neutrality of the *network* providing access to the Internet for the edge users. Independent devices, browsers or operating systems themselves do not constitute a *network* and are not the subject matter of the net neutrality debate. A device may be bundled with a specific operating system tied to a limited suite of applications available for it. However, the fact that certain applications that connect to the Internet are available only for a specific operating system or device is a business decision made by the edge service provider to limit its availability to a specific portion of the Internet is not a net neutrality issue. Just as any edge user of the Internet has the freedom to determine what portion of it they want to reach, any edge service provider also has the freedom to determine the portion of Internet to which it wants to provide services. So long as the TSP/ISP is not able to determine what portion of the Internet should be made accessible to edge users or edge service providers, no net neutrality concerns arise.