

Response to TRAI
Consultation Paper on
Net Neutrality

April 2017

NASSCOM RESPONSE TO TRAI CONSULTATION PAPER ON NET NEUTRALITY

Preamble

Net neutrality does not prevent access providers from managing their networks, and should not prohibit traffic management. However, regulations should ensure that traffic management practices that imposes arbitrary restrictions and discriminatory practices, including blocking, throttling, or altering of specific content, application, or services are strictly forbidden and any such actions should be punishable.

Reasonable traffic management techniques would ideally be on a temporary basis deployed during extraordinary conditions of congestion, and should be targeted towards solving the problem. There should be associated transparency and disclosure requirements when such situations arise.

Traffic management practices should not directly and indirectly bring in any discrimination – price based/ non –price based e.g. source origin or destination of consumption etc.

Therefore, beyond the needs of optimizing the network and addressing traffic hazards through temporary measures, either manually or automatically, no discrimination should be permitted, that can lead to commercial benefits to TSPs and their partners.

Traffic management measures imposing restrictions that offer an unfair commercial advantage to access providers' own services or those of their business partners are anticompetitive practices and should be forbidden under the law.

The scope of TRAI regulations should be entirely focused on ensuring that traffic management practices adopted by TSPs conform to the principles of Net Neutrality. Extension of current jurisdiction of TRAI is neither envisaged nor considered necessary in this context.

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

Response:

Aligned with NASSCOM's previous submissions, we emphasize that regulations are needed to ensure that TSPs do not resort to market distorting practices which go against the principles of Net Neutrality. Given the varying definitions of Net Neutrality worldwide, we present our concept of Net Neutrality specifically tailored to the Indian context for your reference.

Net Neutrality in our view should be characterized by the following attributes

- 1** User to have the unfettered right of making an informed choice in deciding content / services to access
- 2** No discretion to TSPs to censor or block access to any legal content, applications, services, or non-harmful devices or determine how users use internet
- 3** No right of TSPs to throttle lawful internet traffic on the basis of content, applications, services or non-harmful devices. In fact, opening of the content of transmissions other than when required under laid down legal processes, is illegal.
- 4** No right of TSPs to speed-up / favour lawful internet traffic over other lawful traffic in exchange for consideration of any kind.
- 5** Critical that there be a level playing field for all Internet platforms and services including particularly entrepreneurial start-ups so that they are not squeezed out by either TSPs or large/global Internet Platforms and Service providers through anti-competitive tie-ups or practices
- 6** Prioritization of Emergency or any other services as prescribed by the regulator accompanied by public declaration and without price discrimination
- 7** Clear and declared definition of acceptable technical practices by TSPs for management of network traffic in conformity with above principles
- 8** No double dipping by Telecom Service Providers. Charges would be levied only from end customers based on data consumption and not from Internet Platforms and Applications
- 9** Security restrictions as required for ensuring reliable services and lawful demand of security agencies.

The regulatory framework should incorporate suitable provisions to ensure the above and appropriate enforcement mechanisms to deal with any complaints or reported

breach of the principles. As consumers increasingly rely on the Internet and Mobile networks for not only their communication needs but other needs like Banking, transportation, Health etc. we believe that the above principles of open and fair access should be upheld and any violation of these principles should be critically examined and actioned against.

With Digital India poised to transform the country, we believe that consumer and national interests should be paramount, this is all the more imperative

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

- (a) Should certain types of specialised services, enterprise solutions, Internet of Things, etc. be excluded from its scope? How should such terms be defined?**
- (b) How should services provided by content delivery networks and direct interconnection arrangements be treated?**

Please provide reasons.

Response

Internet traffic is the density of data present in the Internet, and Internet traffic measurement is the requirement of both service providers and service users. There are many reasons to measure network traffic including like identifying capacity constraint, session times and traffic volumes for billing and an improved understanding of how to improve network performance

The providers of Internet services or Internet Service providers as per OECD is

"A company which provides end-users with a data connection allowing access to the internet and the associated services (World Wide Web, Email, Chat rooms, Instant Messaging, Internet Telephony and so on)."

TRAI has already identified exception for national emergency and public interest in its February 8th, 2016 order on exemptions in the context of National emergency and areas of national importance, and the same should be exempted under any

regulations related to traffic management. In fact, as in the Feb 2018 order, provisions to expedite such information in case of national emergency and calamity maybe be notified.

Carriers and enterprises today agree on service level agreements (SLAs) to ensure heightened levels of quality. For example enterprises often buy dedicated lines (e.g., T-1, dedicated Ethernet, dedicated fiber, etc.) with associated SLAs for their voice and data traffic in fixed line, to provide an enterprise with heightened quality of service (QoS), security and other guarantees. Such options should continue to be available.

Regarding specified services like IoT - Today IoT solutions do not generate a lot of traffic compared to residential streaming video or other high bandwidth applications. However, as internet-enabled devices increase, IoT devices could use up bandwidth on licensed network when multiple devices are integrated.

Principles highlighted in response above should be the broader tenet.

We believe, Net Neutrality is important for IoT solutions to succeed, and traffic from IoT solutions should not be discriminated against on a licensed network. Further, network performance optimization aligned to Net Neutrality concepts offers a blueprint for how IoT devices and its communication capabilities should be planned, architected, and deployed to minimize burden on the network, by being proactive about improving the efficiency and speed of their data, and also pose it as a source of competitive advantages.

But, a closer analysis of the potential of IoT and in fact solutions being developed and deployed on licensed bandwidth, there are critical real-time applications that will need real time data sharing, failing which it could pose a threat to individual life or even public. For example,

- “Smart” heart monitor sending delayed information of a heart attack can lead to life and death situation.

- Driverless cars - Verizon's telematics experts note that 14 car manufacturers account for 80 percent of the worldwide automotive market and all of them have a connected car strategy, that enable advanced IoT apps like driverless cars which will definitely require seamless access without delays.

Handling bandwidth and access will need to be looked into for such applications where network availability and real time transmission is required, and the Government should consider provisioning for exceptions for certain cases. We would therefore recommend an analysis of such instances and suitable provisions for seamless bandwidth access maybe evaluated for critical applications that could be either in larger public interest but also include individual life threatening situation.

It is also important to point out that IoT devices, mostly low powered, rely on local access technology like blue-tooth or Wi-Fi, and they will in turn require suitable policy intervention to ensure optimized utilization and efficiencies of unlicensed spectrum. However such need not be brought under net neutrality regulations.

Content Delivery Network allows hosting of content closer to their customers, thereby enabling users to connect quickly. Commercial interconnect relationships that allow networks to directly and indirectly include peering and transit relationships. CDN either connects its networks directly with major Internet service providers (ISPs) or co-locates server hardware within ISP network operations.

Typically the CDN-TSP interface usually dwell on conditions of exchange of traffic such as acceptance of traffic, traffic exchange points, direction of flow, how much of traffic - in short it is akin to commercial wholesale interconnections. NASSCOM in its past submission on the issue of differential pricing had clearly outlined that 'proposals by TSPs¹ or TSPs and their partners' should ensure net neutrality is maintained.

However, it is important to note despite CDNs, the responsibility of last mile delivery still the rests with the TSPs and there is no direct link between the CDN and end user. Therefore, we believe that compliance to Net Neutrality principles should rest with the TSPs, and their adherence thereto by TSPs should be enforced by TRAI.

¹ TRAI has regulatory mandate on TSPs only

For any other entities that may be indirectly involved, there are already adequate laws viz IT Act, Competition Act not to mention the conventional IPC, CrPC, etc. that may be invoked by various stakeholders at appropriate forums provided for therein depending on the nature of complaint.

This is in accordance with the principles of Net Neutrality as outlined in the previous response and the reaffirmation that TRAI jurisdiction is limited to TSPs, and other entities such as CDNs need not be brought under TRAI's jurisdiction in the context of ensuring that traffic management by TSPs conforms to the principles of NN.

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.

Response:

Without effective traffic controls, networks are vulnerable to possible congestion when the offered traffic exceeds the network capacity, leading to serious deterioration of network performance.

We recommend a broad based approach that allows for technological choice and innovations in traffic management and data handling.

Traffic management should not involve monitoring of user activity, but simply managing traffic. The regulations should ensure that traffic management practices that imposes arbitrary restrictions and discriminatory practices, including blocking, throttling, or altering of specific content, application, or services are strictly forbidden and if detected be punishable.

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

Response

Traffic management has multiple goals.

- Distinguish different types of traffic and handle each type in the appropriate way. For example, real-time traffic is forwarded with minimal delay while best-effort traffic can afford to wait longer for any unused bandwidth.
- Respond to the onset of congestion.
- Maintain an acceptable level of network performance under heavy traffic conditions.

Principle of Net neutrality does not prevent traffic management practices that are consistent and have an enforceable framework to make sure such practices are reasonable, i.e. situations under which they are warranted and mechanism adopted e.g.

- Unforeseeable transitory congestion - maybe due to equipment failure or other reasons, may require traffic optimization measures. However, operators must be able to prove that such congestion of its network was not foreseeable and that it took necessary steps to correct it.

- Security threat from a sudden attack, malicious actions aiming at altering the global operation of the network, whether intentional or accidental.

Prioritization for stipulated emergency services only that have been declared publicly in the larger public interest, ensuring no discrimination among Internet Platform and service providers of the same category.

Therefore, reasonable traffic management techniques would ideally be on a temporary basis deployed during extraordinary conditions of congestion, and should be targeted towards solving the problem. There should be associated transparency and disclosure requirements when such situations arise.

Net neutrality in any context should stand for

1. Unfettered user right of making an informed choice in deciding legal content / services to access
2. No discretion to TSPs to censor or block access to any legal content, applications, services, or non-harmful devices or determine how users use internet
3. No right of TSPs to throttle lawful internet traffic on the basis of content, applications, services or non-harmful devices. In fact, opening of the content of transmissions other than when required under laid down legal processes, is illegal.
4. No right of TSPs to speed-up / favour lawful internet traffic over other lawful traffic in exchange for consideration of any kind.
5. Critical that there be a level playing field for all Internet platforms and services including particularly entrepreneurial start-ups so that they are not squeezed out by either TSPs or large/global Internet Platforms and Service providers through anti-competitive tie-ups or practices
6. Prioritization of Emergency or any other services as prescribed by the regulator accompanied by public declaration and without price discrimination
7. Clear and declared definition of acceptable technical practices by TSPs for management of network traffic in conformity with above principles

8. No double dipping by Telecom Service Providers- Charges levied only on end customers based on data consumption and not on Internet Platforms and Applications
9. Security restrictions as required for ensuring reliable services and lawful demand of security agencies.

Traffic management practices should not directly and indirectly bring in any discrimination – price based/ non –price based e.g. source origin or destination of consumption etc.

Therefore, beyond the needs of optimizing the network and addressing traffic hazards through temporary measures, either manually or automatically, no discrimination should be permitted, that can lead to commercial benefits to TSPs and their partners.

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]

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

- (a) **Emergency situations and services;**
- (b) **Restrictions on unlawful content;**
- (c) **Maintaining security and integrity of the network;**
- (d) **Services that may be notified in public interest by the Government/ Authority, based on certain criteria; or**
- (e) **Any other services.**

Please elaborate.

Response:

We believe that the situations outlines in (a) to (d) would require exceptions under the Net Neutrality and Traffic Management principles, to ensure support and help during emergency and life threatening situations, as well as restriction and weeding out of unlawful activities.

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?).**

Response:

Traffic management fundamentally involves a balance between conflicting objectives: statistical sharing versus isolation.

We recommend suitable technology working groups be set up to look into each of the practices and suggest the way forward.

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?

Response:

Traffic management practices that are reasonable and consistent should be implemented in a transparent manner. Therefore full disclosure to the regulator would be essential. We therefore believe (b) is important and should be statutory.

On information to user, making available traffic management policies and sharing information on how telecom services are affected by traffic management with the users is important and necessary. Therefore option (a) is also necessary.

However, given that traffic management and network performance is measured from a network provider's point of view, e.g. end-to-end or hop-by-hop performance, may be aggregated over the entire user population, average end-to-end packet delay or fraction of packets lost per hop observed over an interval of time. But this will be of little or no relevance to the consumer. On the other hand, QoS metrics are oriented towards a user's end-to-end experience e.g. end to end packet delay time less than 10 sec or a certain packet loss rate that users will find more meaningful, depending on their QoS requirements. The nature of information shared will therefore have to be suitably defined by TRAI, depending on the target group.

Further, we believe that the traffic management policies should be shared with the user and regulator on a one-time basis when a practice is introduced or when a new user is added. Thereafter a need to share information on traffic management policy and practice afresh would be triggered only if

1. There is a major change in traffic management policy OR
2. In case of a major event that had a significant impact on user experience.

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]

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

- (a) **Which body should be responsible for monitoring and supervision?**
- (b) **What actions should such body be empowered to take in case of any detected violation?**

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

Response:

The TRAI should notify regulations that are based on high level principles, as it has done in the past, but the scope should be limited to TSPs and their violation of Net Neutrality to the extent it can be regulated by TRAI within its current ambit.

Issues that extend beyond the current jurisdiction of TRAI, should be remitted to other relevant regulatory authorities like Competition Commission, MEITY, etc.

Alongside, we recommend self-regulation as against a regulatory 'pre-approval' regime.

However, powers to monitor, further strengthened with provisions for calling for or collection of information, taking into cognizance complaints by third party and whistle blowers as well as robust dispute handling mechanism should be made available.

The regulator should be empowered to play a key role in evaluations and suggest strict action on proven violation, and issue directions to remedy violation.

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).**

Response:

A combination of all the above is recommended. While (a) should be made a statutory requirement, both (b) and (c) should be on a voluntary basis.

One of the critical challenges that a regulator will face would be accuracy of information and its evaluation. The regulator should have necessary tools and expertise to monitor and analyse details shared, to be able to verify disclosures made and identify any missing information, instances of violation of NN, etc.

Further, a suitable process to request for and receive feedback from users, third party and to involve experts in analysis of complaints should be in place. This will help the regulator issue suitable directions for implementation.

**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]**

- (a) What should be its design and functions?**
- (b) What role should the Authority play in its functioning?**

Response:

There should be a forum to constantly scan the environment for any violation of Net Neutrality framework. The Authority should continue to organize open house consultations for this purpose as it has done in the past.

The collaborative mechanism adopted by TRAI and DoT through its consultation process, can be further extended by constituting an advisory board across stakeholders to suggest specific operational aspects.

Further, an advisory board necessarily should be supported by technology working groups and Technology evaluation committees. Based on the recommendations of the advisory group, the TRAI and other relevant regulator can then notify regulations and issue directions.

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

Response:

Violations of Net neutrality principles in the country and key incidents globally should be tracked by the regulator or an organization identified for this purpose. An Annual Report should be prepared or directed by the regulator who can then make the content public, as and when deemed appropriate.

Based on the trends, the advisory group and other stakeholders may be consulted on issues.

There should be a well-defined mechanism where an advisory group of stakeholders can also suggest to TRAI and other relevant regulatory authorities, as per their jurisdiction like MEITY, Competition Commission etc. aspects of regulations that require discussions, changes etc.

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]

Response:

Enforcement of NN rules by TRAI rules are expected to focus on TSPs/ISPs and internet users, and expanding the scope is not advisable. Any violation beyond this should go to other regulator as per law.

As outlined above in response to Q 2, Net Neutrality not only assures an equal opportunity but also offers a blueprint for how solutions should be planned, architected, and deployed to minimize burden on the network, by being proactive about improving the efficiency and data speed.

With increasing user requirements of better services, we believe that the product developers and service providers would be under constant pressure to improve performance, and inherently inefficient solutions would be weeded out by market dynamics.

Therefore, a collaborative standards based approach should be adopted. These standards should be global and encourage interoperability for maximum ease of adoption.