TATA

12th April 2017

Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
(Old Minto Road)
New Delhi – 110002

Kind Attn.: **Shri Asit Kadayan**
Advisor (QoS)

Subject: **Consultation Paper on "Net Neutrality"**

Dear Sir,

This is in reference to your Consultation Paper issued by the Authority dated 4th January 2017 on **"Net Neutrality".**

As desired, we hereby enclose our response to the questions raised in your above mentioned Consultation Paper. We hope our response will be given due consideration. We shall be obliged to address any further queries from your good office in this regard.

Thanking you and assuring you of our best attention always.

Yours sincerely,

Satya Yadav
Addl. Vice President – Corporate Regulatory Affairs
Tata Teleservices Limited
And
Authorized Signatory
For Tata Teleservices (Maharashtra) Limited

Encl: As above

TATA

TTL's Response to the TRAI Consultation Paper on 'Net Neutrality'

1) **What could be the principles for ensuring non-discriminatory access to content on the Internet, in the Indian context? [See Chapter 4]**

TTL RESPONSE

There are multiple factors driving the net neutrality debate, the way in which governments are addressing net neutrality, the requirements of the Industry, the end-user and the other participants such as the content providers. The topic of net neutrality is not limited to a technical debate and brings together a number of issues including the right to access, fair competition practices, among others.
The authority can protect net neutrality and consumer choice while also continuing to foster innovation by adopting a balanced approach. Non-discrimination is an important component of net neutrality.

However, differential treatment is not inherently discriminatory as long as any additional offer includes any content that meets the same, uniformly applied technical requirements. Also, when a given arrangement between a TSP and content provider is available to all TSPs on the same terms and conditions. There has to be transparency on the speeds of the content that flows over networks. Non-discrimination has to be followed by all the stakeholders in the end to end value chain. Non-discriminatory access to content be guided by the following principles:

i) Not discriminating Internet traffic based on similar type of content or applications not favouring self generated content or traffic over another by the service provider or even by aggregator for any consideration
ii) All similar type of content to be treated equally,
iii) Service providers should not to intentionally slow down the speed of some select content providers or speed up others
iv) not providing end-users free or subsidized access to their own content or content provided by 3rd-party content providers who may have paid the TSP to subsidize the content
v) TSPs should not undertake harmfull practise like blocking , throttling or improper priotitization (paid or otherwise) except for below reasons:
   (1) Implement a Fair Usage Policy (FUP)
   (2) User's IP is generating harmful / malicious / unlawful content
   (3) User's IP is infected compromising security of the network

Deep Packet Inspection should be allowed for specified reasons mandated by law and that should be made transparent. Also, lawful deep packet inspection is to be permitted for network management and efficient traffic flow requirement purposes by the service provider.

Differential treatment, however, is not inherently the same as discriminatory treatment. Differential pricing based on bouquet of Product & Service opted by the customer can be offered in a non-discriminatory manner that is both consistent with the principles of net neutrality and beneficial to consumers.

We also believe that rules and policies for all stakeholders and participant in the entire end to end chain/OR similar industries should be uniform and level playing.

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?**

TTL RESPONSE

While the open internet is the primary reason for setting up network infrastructure, the networks could be used to access specialised services that are not part of the internet at large. This includes enterprise solutions, M2M Communication, IoT, and content delivery networks. For example, a TSP can host content from a particular content service provider, allowing for better access to that content on that network.

TSPs have a need to do efficient traffic management activities which cannot be linked with net neutrality violation, provided those activities do not result in faster alternative paths for any affiliated services/ applications or blocking or throttling for specific classes of content and services.

The development of the internet has significantly altered the day to day operations of businesses across the country; including how they communicate with each other and their customers. The internet is critical to their operations and in many cases, Information needs to be transmitted and accessed on a real time basis. Considering the requirements of Businesses, we believe that solutions provided to them should be excluded from the scope of the net neutrality discussion.

TSPs have an obvious need to enter into business arrangements to promote Internet connectivity. IT should not be seen a violation of neutrality principals, provided such arrangements do not involve blocking or throttling users' ability to connect to the broader Internet with no additional terms and conditions.

Additionally, at times solutions/ services may also be deployed by the Business for its employees (or Closed User Group, which may include employees, partners, suppliers, 3rd Party agencies) either on an Intranet or the Internet and could include access to:

- Intranet Applications
- Customer Applications hosted on the Internet

- Company WAN
- Machine to Machine Connectivity
- Internet of Things
- Private Cloud
- Access of Data Centre infrastructure over the Internet / secure network

b) How should services provided by content delivery networks and direct interconnection arrangements be treated?

TTL RESPONSE

Content Delivery Networks allow internet companies to distribute their content geographically, so that download speeds are better and the end-user experience is significantly enhanced. CDNs make the surfing experience better for everyone, by better distributing content to speed delivery to everyone. CDNs benefit all end users and they definitely don not selectively throttle content as also mentioned in some context in response to preceding questions and thereby in our view do not violate the fair and universally accepted / practiced principles of net neutrality.

Direct Interconnection / Peering arrangements between TSPs and Content Providers should be permissible only under the following circumstances and as also reflected in our other replies above;

1) Access to the content is not free of charge.
2) Content is not prioritized over other similar content provided by a competing content provider.

It is our suggestion that the scope of Content providers and CDN providers be clearly defined and regulated so as to ensure complete transparency.

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.

TTL RESPONSE

Different kinds of content require different kinds of connectivity. For example, video or VR content needs a high speed connection. Gaming content does not require high speeds, but low latency and constant connectivity are important. TSPs need to manage the traffic in various ways to ensure that all the users are getting a uniform quality of service, despite consumption of different kinds of content.

Drawing from the European Union's regulations, the Broad approach refers to guiding principles like proportionality, non-discrimination, transparency and absence of commercial considerations that can be used to define the bounds of reasonableness. It would be extremely difficult to define a board range of reasonable TMPs as the internet is evolving by the day and this approach would lead to ambiguity.

A negative approach or exclusion principle is more preferred as it would lead to clearly defining TMPs which are unreasonable.

While it is acknowledged that the approaches have to safeguard the interests of the user, the service providers at the same time have to genuinely handle the traffic loads. Designing the network for peak use throughout would mean a lot of wasted capacity most of the time and that would be commercially unviable.

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 users choice and without any arrangement between a TSP and content provider, be treated?

TTL RESPONSE

In order to be considered to be "reasonable", traffic management would have to be based on objectively different technical Quality of Service (QoS) requirements of specific categories of traffic. Categories of traffic could be defined, for example, by reference to application layer protocol or generic application type, but only in so far as:

a) This requires objectively different technical QoS;
b) Applications with equivalent requirements are handled in the same category; and
c) The justification given is relevant to the category of traffic in question.

As mentioned above, if traffic management is prescriptive it will hinder the development of networks. Defining the contours of what is permissible under TMP would constitute over-regulation in our view and as such detrimental to an industry that is fundamentally dynamic in nature.

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

TTL RESPONSE

Management of traffic during times of congestion is a win-win as the majority of subscribers continue to have a perceived and good quality QoS as logically reasonable and the access network lifetime is extended, allowing network investments to be made in other areas of need. In an access network environment, there are several areas of 'narrowly-tailored' that might be technically considered for addressing subscribers who are causing disproportionate congestion. These include:

- Network type
- How access nodes and links interact
- Subscriber density per access node
- Subscriber demographics per access node
- Backhaul network capacity
- Unforeseeable events

So far, Traffic Management has been guided primarily by the principles of first-come-first-serve management of traffic and more advanced ways of shuffling traffic through the networks.

Alternative traffic management is required for circumstances and as such is based on categorizing the traffic based on certain criteria like exemplified below (amongst others):

a) congestion management measures
b) Requirements of Enterprise customers

An important point to be considered is whether encrypted traffic is treated at par with normal traffic. This is specifically applicable in the case of solutions provided in the Enterprise segment. In our view, the following should constitute the negative or exclusion list as was indicated in our reply to Q1

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 Any other services. Please elaborate.

TTL RESPONSE

Yes. Situations which can be classified under above categories may have severity, urgency, security concerns etc attached to it and hence it is vital to differentiate such situations and treat them as exceptions.

Risk of not having them as exceptions may result in a delayed response in an adverse situation, which would be unacceptable to the parties involved.

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?).**

TTL RESPONSE

All the mentioned items (Blocking Throttling Prioritizing / Preferential Treatment), the control and treatment has to be safeguarding national interest and therefore have to be viewed and considered in proper context and with rational background by only the authorities exercising the legal rights in terms of :

- Protecting consumer rights including privacy rights.
- Promoting fair competition.
- Administration of law with respect to established ACT.
- Tools and techniques to detect the anti social activities.

Smooth transactions, transfer and interaction taking place through social media or otherwise in a "clear and conspicuous" manner.

Critical issues involving Security requirements (including Cyber Resiliency), Privacy requirements and Lawful Interception requirements.

This also needs to be viewed in terms of preventing or detecting objectionable, obscene, unauthorized or any other content message, spam blocking, tightening of remote access connectivity beyond national boundaries and providing adequate protection and monitoring of Infrastructure from various attacks including DDoS etc.

In light of that the following definitions may be considered. However, these could be redefined if need be, for those to be seen and perceived in right context and in line and harmony without circumventing the other replies given by us to the questions asked by TRAI in this the paper and the operational needs of the service provider in some exceptional / exclusive circumstances.

- Blocking – Any unlawful obstruction to access a particular URL / URI of Non-Commercial , Commercial site and the related services on / by the same in the form of content, by any inter-mediatory in exchange for commercial considerations / anti-competitive agreements either with a third party or otherwise

- Throttling – Any intentional slow down, restrict or Discriminate access a particular URL etc. by the service provider in exchange for commercial considerations
- Prioritising / Preferential Treatment - Any intentional acceleration of various formats of commercial or similar un-socially motivated data stream or content transfer rate including the time taken in accessing (which could feasibly be in direct control of the service provider) a particular URL / URI etc.

Tests, Thresholds and Technical Tools as also available, referred or in use as global best practices can be adopted for monitoring, detection and deployment. Such, thresholds tools and test methodologies can be fairly used on, with level playing field principles, equally applicable for all the participating stakeholders in the end to end value chain in a correlated and corroborated way.

For example if the comparison of one stakeholder is to be done with that of another stake holder for an app, is perceived to be getting throttled in a particular access service providers network, then verification of the logs or KPI markers of only of the particular service provider shall not suffice. The findings of the analysis logs of the App provider needs to be done for correlation and corroboration including also other intermediary NLD / ILD networks in the value / supply chain. The monitoring authority may crowd source the speeds / access of various sites from the connections provided by various service providers.

Similarly, some unbiased and neutral non-influencing APPs can be developed which can be used to test various URLs / URIs / IP addresses from the connections provided by service providers in appropriate and normal environment avoiding extreme cases which give exceptional false positive indicators / results in extraneous conditions beyond their controls.

- Any such tests may be carried out when really required for over a longer periods and for large samples period to arrive at a credible suspicion of violation of NN principles if any
- Similarly, for time taken to access, considerable analyses over time and set of circumstances, the same could become the benchmarks if any for such accessing/ streaming of particular content.
- Only based on the outcome of collection of data, its analysis, correlation and corroboration can the stakeholders be judged as a violator of NN principles. This would take much longer time, experience and fair training even to define candidates /items / incidents fit to be defined as NN violations or for that matter violators.

- For any such measure the content provider's setup too has to be mandated to have adequate capacity and use the CDN services of the domestic service providers.
- Sometimes a typical types of services could be judges at Internet POP gateways, i.e., between Boarder Gateway router and Internet gateways.
- Due to advancement of technologies, the tools may possess intelligence to filter unwanted/unneeded traffic to reduce traffic monitoring load.
- However, everything comes as a cost and the real need has to be established and at the same rime cannot be considered as a routine activity. Such automations also need rime and huge costs as well as work flow challenges

The authorities should not just ask to telecom operators to put such dedicated and restricted monitoring systems in the service provider's premises and at their costs. It involves all the stakeholders end to end in the eco system and as anyone in the chain may be the ultimate so called defaulter after all such investigation, if at all
Mechanism and technical challenges required for every type of traffic and content is somewhat different in real practice or time

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?

TTL RESPONSE

In Indian context, disclosure to the Regulator would be recommended option. The mode would be disclosure in a standard template published to the Regulator every quarter. The information disclosed would include:

a) Plans offered in the market-place (already being done)
b) Average QoS performance across wireless and wireline networks (already being done)
c) Exceptions towards TMPs and the reason for the same. This should be disclosed to customers at the time of signing up or as an when its implemented

We believe that solutions offered to the Enterprise Segment should not be under the purview of net neutrality and hence excluded from the scope of this disclosure.

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]**

TTL RESPONSE

While the template is broadly acceptable, certain information being sought is already being provided. The finalisation of the Information Disclosure Template requires a more detailed discussion between the regulator and the TSPs. In addition, we believe that specialised services to the Enterprise Segment should not be within the scope of the disclosures.

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?**

TTL RESPONSE

Any licensing or Regulation which cannot be implemented or monitored effectively is not ideal and will not be a recommended solution. It is our view that it will be very difficult to implement a cost effective solution which will allow any agency to effectively monitor the conditions under which there was non-compliance.

Non compliance with defined parameters could be a result of numerous factors not restricted to the TSP. The Regulations which are currently in place are effective enough in terms of ensuring the larger public internet and hence we believe that no additional license/ Regulation need to be bought forth.

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).**

TTL RESPONSE

TMP is complex and monitoring the implementation poses significant technical difficulties. Even if technical solutions are implemented at great cost to the TSP, there is no guarantee that these solutions will meet the needs of regulators. There are numerous reasons why technical solutions will not meet the requirements:

a) User experience is combinations of Internet Access and Applications/content that the user is attempting to access. What if the Application provider is facing technical issues which could impact the user experience in terms of :
   i) Speed – slow or no access
   ii) Download – slow or denied

It both of these scenarios, it can be misunderstood at times that the TSP is discriminating while that may not be the case at all. From an end user perspective, it would be difficult for them to differentiate and identify the root cause of the issue. Best practices are followed in any case.

The proliferation and dynamic nature of new technologies will also make the implementation difficult.

It should be ensured by the Authority that the implementation of the recommendations is the joint responsibility of all the stake holders and not only that of the TSPs. There should be a common pool of financial resources available for the TSPs to implement any futuristic recommendations. TSPs alone should not be burdened with the significant financial impact of this decision.

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?

TTL RESPONSE

Most important principle for a collaborative mechanism to work is only if all stakeholders are governed by the same policies and guidelines. Content is provided by ASPs and the end user will deliver judgement on the user experience based on whether he is in a position to access the content or not.

For example if it is found that the TSP is responsible for a degraded experience, then the Regulator may resort to penalise the TSP but there is no such provision or intent to penalise the content provider if they are responsible for the degraded user experience.

While TSPs are governed under the UASL, Content providers should also be governed to ensure good QoS.

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]**

TTL RESPONSE

We believe that an expert Advisory Board is best suited to ensure that the NN policy is updated on account of evolution of technology and use cases. This Advisory Council would consist of

a) IT experts
b) Representatives from Industry
c) Representatives from Regulator

If the scope of the NN framework brings the OTT and ASP providers under the framework of the regulation, then it would be advisable to include them in the Advisory Board as well.

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]**

TTL RESPONSE

In the past few years, there has been an exponential increase in the internet traffic, with new services and applications that have appeared. In view of this huge growth, it has become clear that stringent levels of QoS that have been appropriate in the past may need more fine tuning.

The quality of the internet service is not a result of the bandwidth provided by the TSP. It is a result of a multiple factors such as the type of device, the browser being used to access the internet over the device, the OS version and the type of content being accessed. All these factors contribute to QoS and it's important that they be considered while determining QoS.

In addition to this, Data Networks today also enable IOT, M2M and other applications which need different treatment which require completely different type of QoS parameters.

If a complaint comes in, it would have to be evaluated not just by the throughput provided by the TSP, but factors like device, application, OS, browser, etc would need to be considered and that's where the matter becomes complicated.

a) It can be misunderstood that the TSP is discriminating if the Application / Content / Service itself has a issue
b) Slow speed / download time could be a result of OS and application bugs being faced by the user at that time OR the ASP data centre may not be sized to handle appropriate traffic
c) The device may be infected with malware which could impact the user experience

All of these issues contribute to the user experience and it would be very difficult for the Regulator to determine the exact cause of the reason at any given point of time. We believe that QoS in the context of Net Neutrality would be extremely difficult to determine and hence should not be included in the scope.