12th April, 2017 New Delhi

To,

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

2. Shri Asit Kadayan
   Advisor (QoS)
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

Re: RESPONSE TO NET NEUTRALITY CONSULTATION, TRAI, 2017

Dear Sir,

The TRAI Consultation Paper on Net Neutrality is a commendable step towards achieving a free and open internet.While presenting this response to the consultation, due care has been taken that the suggestions made herein are in line with internationally accepted standards of 'free internet', and are also tailor-made to India's access and quality of service requirements.The response has been divided two parts for ease of perusal: *Part I* contains a *summary of the recommendations* and *Part II* is the *explanatory memorandum* which contains *reasons* along with the recommendations.

Part I: Summary of Recommendations

Q.1 What could be the principles for ensuring nondiscriminatory access to content on theInternet, in the Indian context?

Response

With regard to the contextual needs of India and the relevance of technological, economic and legal considerations, it is recommended that the following factors qualify a non-discrimination rule aimed at preserving network neutrality as far as possible:

- **Like traffic be treated alike. Only different types of traffic may be treated differently.** i.e. it should be service provider and origin/destination agnostic. For example, all service providers of the same type, such as video streaming or VoIP, may be prioritized when there is congestion. Emergency services may be of different varieties such as tele-medicine, VoIP calls to police forces etc. however they may be treated as a single class of emergency services.

- **Any discrimination or differentiation of traffic be conducted out of necessity and not commercial considerations and should not be anti-competitive**. For example, differentiation of traffic is acceptable in exigencies and during peak hours if there is congestion but not for commercial considerations such as an agreement between content providers and TSPs. Further, packets that are not time and lag sensitive, such as emails, should not face any discrimination in the network, whereas other services such as video and VoIP be prioritized when the necessity arises.
- To ensure that differentiation of traffic is not done without necessity it should always be **limited in time and the criterion of necessity be provable through empirical data**.
- Any stipulation made in this respect, irrespective of whether these recommendations are considered, should be **flexible and subject to regular review** and updated based on stakeholder feedback to ensure that such stipulations keep pace with change in technology. For example, when the broadband infrastructure is robust enough to support bandwidth demand, there may not be any need for traffic management.

It is further recommended that:

- TRAI study and conduct a consultation to determine incentives for certain stakeholders, such as small ISPs, beyond the extant framework. The goal of such an exercise is to promote competition and innovation and deter circumvention of the goals of net neutrality. For example, without adequate competition among TSPs there is a danger that incumbent internet providers may circumvent necessary investment for expanding the network infrastructure by relying excessively on traffic management practices to handle congestion.

Q.2 How should “Internet traffic" and providers of “Internet services" be understood in the NN context?(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

(a) It is recommended:

- Establish threshold QoS standards for public internet that should not be violated in providing for specialized services.
- Specialized services should be defined narrowly and network utilization by TSPs of specialized services vis-à-vis public internet should be monitored.
- No specific service or conception should be included in the exception such as Internet of Things as it may be provided over the internet or through a specialized service.

(b) It is recommended:

- CDNs enhance efficiency and quality and, therefore, should be encouraged. A framework should be established for transparency in the deployment of such technologies and arrangements. This may be subject to further consultation by TRAI.

- Interconnection is beneficial to all stakeholders and should be left to the market rather than regulation.
- Under no circumstances should interconnection/peering be prohibited, as done by NIXI.

Q.3 In the Indian context, which of the following regulatory approaches would be preferable: (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

It is recommended that:

- There should be a hybrid approach with a broad stipulation on reasonable TMPs and a narrow approach prohibiting some kinds of TMPs.
- TMPs refer to Reasonable Network Management practices which may be in the form of throttling or prioritization.
- It should be application agnostic.
- Unreasonable TMPs include commercial arrangements, anti-competitive practices and arrangements that violate application-agnosticism
- Blocking should only be allowed for illegal activities as detailed in our response to Question 6.

Q.4 If a broad regulatory approach, as suggested in Q3, is to be followed: (a) What should be regarded as reasonable TMPs and how should different categoriesof traffic be objectively defined from a technical point of view for this purpose?(b) Should application-specific discrimination within a category of traffic be viewedmore strictly than discrimination between categories?(c) How should preferential treatment of particular content, activated by a users choiceand without any arrangement between a TSP and content provider, be treated?

Response

It is recommended that:

- Reasonable TMPs should necessarily be application agnostic.
- It may be useful to consider user preferences. However, there are no ready examples of enabling a consumer choice based model. Thus, the TRAI should hold a consultation to determine the same.

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

Response

- This requires further study and should be subject to future notification.

Q.6 Should the following be treated as exceptions to any regulation on TMPs? (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

The following recommendations may be considered:

- The resultant network neutrality stipulations should allow emergency situations and services to be considered a reasonable TMP. However, it should also be specified in the relevant provision that the service so exempted must be mandated through a lawful order given by an appropriate authority or competent court of law and only after defining it narrowly. Further, the provision so contained in a net neutrality instrument should also be defined narrowly, considering the following factors:
    - Such emergency services should be caused by exigencies which may be natural such as earthquakes, wherein relief services may be prioritized, or man-made such as spread of malware.
    - It is critical that such an exception should not be used to block or throttle internet services for case that may be mandated by an appropriate order, but are not an emergency. For example, mobile internet was blocked for four hours across Gujarat in February 2016 to prevent cheating in a state entrance exam.[1] This would not qualify as an emergency service under the net neutrality framework.
    - Considering the nature of emergency situations the *ex post facto* orders may be considered lawful.
- Unlawful content may be blocked only if mandated through a lawful order given by an appropriate authority or competent court of law, after defining it narrowly and only till such time the unlawful activity continues. For example, if a url/website is blocked for obscene content, it should be done only through an executive or court order and only till such time the objectionable content is available on it.
- It is essential to consider maintenance of security and integrity of the network as a reasonable TMP. However, the TMP must be proportionate to the threat and should only continue for the time-period necessary. Further, the instances of using TMPs for maintenance should be documented within a reasonable period of time and should be made available for regulatory/ public scrutiny as appropriate.
- If other services are notified as exceptions in public interest, since the phrase 'public interest' does not have a overarching definition, it should be done only on the basis of a defined category of services which may include providing essential welfare services such as transfer of subsidies. However, other initiatives by the Government that may benefit the public but is in economic competition with the private sector should not be exempted under the TMP framework.
- There should be no generic provision to allow 'any other services' for exemption.

Q.7 How should the following practices be defined and what are the tests, thresholds andtechnical tools that can be adopted to detect their deployment: (a) Blocking; -(b) Throttling (for example, how can it be established that a particular application isbeing throttled?); and(c) Preferential treatment

[1]Freedom House: Freedom on the Net 2016 - India, November 2016, https://freedomhouse.org/sites/default/files/FOTN%202016%20India.pdf

(for example, how can it be established that preferentialtreatment is being provided to a particular application?).

Response

It is recommended that the following aspects be considered while defining blocking and differential/preferential treatment:

- Blocking refers to the practice of obstructing access to one or more service(s) of one or more consumer(s) by using traffic management practices or other means. Blocking should only be allowed in furtherance of a lawful order such as by an appropriate authority or by a competent court of law.
- Differential/ Preferential treatment includes throttling and prioritization wherein one or more service(s) is made less/more accessible in comparison to other services by reducing/ improving the quality of service or by other traffic management practices and is only reasonable if non-discriminatory as given in our response to Question 1.

Based on our findings, we recommend the following initial regulatory efforts with regard to TMP detection:

- Before an indigenous TMP detection system is developed, TRAI should seek to identify and authorize testing tools to facilitate official monitoring of unreasonable TMPs. Tools offered by open systems such as Ookla, Glasnost and Mlab and private entities such as SamKnows, can be useful for this initiative.
- Simultaneously, there must be a comprehensive stakeholder consultation by TRAI with ISPs, consumers, public policy entities, academic and industry experts, etc. to collectively determine and standardize an appropriate TMP detection regime, including:
    - To develop detection/ measurement parameters such as download speed, upload speed, jitters, packet loss ratio, latency, etc. Technical recommendations, standards, technical specifications and guidelines from international bodies such as the ITU, International Organisation for Standardisation ('ISO') and the International Electrotechnical Commission ('IEC') can be used as a point of reference.[2] The final decision with respect technical criteria should be made after appropriate consultation with technical experts.
    - To develop an official measurement/ monitoring system which fits India's internet ecosystem, appropriate consideration must be given to parties who have relevant experience in the development of such systems, such as IIT Delhi. Moreover, TRAI may analyse national measurement systems/ applications by other jurisdictions such as Hungary, France, Croatia, Austria, Serbia and the UK and assess the feasibility of adopting their detection tools to India's net neutrality regime.
    - To determine if a software based monitoring mechanism will suffice or if a hardware based mechanism is required as well.

[2]Milan Jankovic, *Regulatory challenges related to the Quality of Service and Experience*, International Regulatory Conference for EuropeRegulating Electronic Communication Market26-27 September 2016, ITU, http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Regulatory%20Conference/MILAN%20JANKOVIC.pdf

Q.8 Which of the following models of transparency would be preferred in the Indian context:(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 publishsuch information?

Response
It is recommended:

- A **mixed approach** be adopted wherein –
    - The consumer and public are kept informed of all the details required to make an informed decision such as QoS, expected speeds, contention ratio, traffic management practices etc. without compromising readability due to technical details.
    - The regulatory disclosure is more detailed in nature and contains technical information regarding frequency of congestion, reason for using traffic management, type of TMP used etc.

With regard to the trigger, mode and frequency for publishing such information, it is recommended:

- **Public** - The disclosure must be made to the public along with the display of the offered data plan and services. For example, the updated disclosure should be available at point of purchase, along with advertisements and along with any other communication to the public regarding data plans and other services. Additionally, all such disclosures should be made in at least two languages including English and the major regional/state-level language.
- **Consumer** – The consumer should be informed specifically every time there is an update in the practices of the TMP through the mode of communication opted for by the consumer (email, post, phone number etc.). Additionally, all such disclosures should be made in at least two languages including English and the major regional/state-level language.
- **Regulator** – The regulator should receive disclosures at the end of every month with a summary of the congestion experienced and TMP used by TSPs in that month. Further, the regulator will also be kept informed of any updates to the disclosures provided to the public and consumers. The information should be available for perusal by the public on the TRAI website. However, this does not include information that may compromise proprietary secrets or confidential information.

Q.9 Please provide comments or suggestions on the Information Disclosure Template atTable 5.1? Should this vary for each category of stakeholders identified above? Pleaseprovide reasons for any suggested changes.

Response
While the format suggested by TRAI is appropriate, there are omissions noticed that may lead to vague or partial communication of information, as follows:

- Under 'Other Terms and Conditions' the download limit, upload limit, data usage caps and fair usage policies should all be mentioned separately to avoid confusion and for better consumer readability.

- Under 'Application Specific Traffic Management' ('Service Limitations and Traffic Management') there should be an additional parameter to disclose bandwidth throttling as follows – "*Are any services, content, applications or products always **throttled** on this plan?*"
- There should be an additional parameter for specifying traffic management practices for any other reason as follows – "*Are TMPs deployed for any other reason? Please specify the reason, the services affected and the type of TMP used (blocking, throttling, prioritization).*"
- There should be a glossary of terms listing out definitions of technical words (such as TMP, latency, blocking, throttling, prioritization etc.) at the end of the Template for the benefit of the consumer.

Based on the comparative analysis it is recommended:

- Clear ***accessibility*** requirements be set out. Specifically:
    - A separate template be made for each plan or cluster of similar plans but not of all or different types of plans (entry level, unlimited etc.).
    - Each ISP should display the Template at point-of-sale and where the plans are displayed on its website rather than under other topics like legal, community etc.
    - A complied list of Templates from different ISPs be made available on the TRAI website and website of any co-regulatory or other body so empowered linking the actual URL containing the Template rather than the website of the ISP.
- A clear ***timeline*** be set out for the publishing of templates, including:
    - An annual **date** when the availability and up-to-datedness of the Template can be ascertained. There should also be random checks to ensure the continued availability of Templates.
    - If they Template requires updating to reflect changes/additions in plans the same should be intimated to the TRAI or any other body set up for this purpose such that it may be verified and reflected in lists complied by TRAI or any other body empowered to do so.
    - The Template should include a date to reflect the date of the last update.
- The Template so displayed by ISPs should be subject to ***independent and regulatory audits*** *(see also response to Q.11)*, preferably both, and this information be displayed by ISPs on their Template, as follows:
    - The independent audit may be conducted by a designated organization empaneled for this purpose that has the capacity to verify based on empirical and statistical testing. This can be a civil society organizations, a technical institution such as an information technology university or a multi-stakeholder body.
    - The regulatory audit may be conducted based on information received by the empaneled agency or multiple agencies as well as based on information independently obtained by the regulator. This can be done by TRAI, a co-regulatory or other body set up empowered to do so or a combination of the two.
- It is recommended that a tabulated-format for publishing traffic management of specific services or type of traffic be appended at the end of the Template, such as the one used in the KFI, with slight modifications as follows:

Sl. No.	Traffic Type	Blocked	Slowed Down	Prioritized	**Reason** (eg. peak time, congestion, emergency)
1.	Peer to peer				
2.	News				
3.	Browsing/email				
4.	VoIP (Voice over IP)				
5.	Gaming				
6.	Audio streaming				
7.	Video Streaming				
8.	Audio download				
9.	Video download				
10.	Other download (please specify)				
11.	Instant Messaging				
12.	Background/ Software Updates				
13.	Other (please specify)				

Q.10 What would be the most effective legal/policy instrument for implementing a NN framework in India? (a) Which body should be responsible for monitoring and supervision?(b) What actions should such body be empowered to take in case of any detectedviolation?(c) If the Authority opts for QoS regulation on this subject, what should be the scopeof such regulations?

Response

(a) The TRAI should be responsible for monitoring and supervision informed by the recommendations of a collaborative body.

(b) While the TRAI and TDSAT are the most appropriate forums to adjudicate disputes, and impose penalties for net neutrality violations the only bench in existence is in Delhi. Further, the TDSAT is only empowered to hear a class of consumers and not an individual. Thus, it is recommended that:

- TRAI and TDSAT should be the appropriate forum for dispute settlement and imposition of penalties under the net neutrality framework. The penalty may be in the form of daily fines till the cessation of the violation. If the violation crosses a threshold then the case should be escalated to the Department of Telecommunications who can suspend or cancel the license of the incumbent. For example, the threshold may be three violations before escalating to the DoT or violations extending to more than 30 days cumulatively in a year.
- Considering the logistical and other limitations of the TRAI and TDSAT the jurisdiction of other appropriate forums, such as the Consumer Forum and Competition Commission, should not be ousted.

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:
(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) It is recommend that:

- If TRAI adopts interim measures for TMP detection using open source measurement systems, they must clearly endorse the tools which are officially accepted as legitimate by way of notification.
- Moreover, TRAI may be required to create a database where overall measurements are stored and analyse to determine the widespread TMP practices of ISPs. If TRAI chooses to publish "raw" data from any official measurement tool/ monitoring system, developed in the future, for the sake of transparency it must be ensured that privacy of users is not compromised.
- The publication/ disclosure of TMP practices must not be buried within service agreements or in complex technical language. There must be easily traceable, and enumerated in comprehensible language. To this end, TRAI must explore if such disclosures of official TMP policy are published in multiple languages including English and the major regional/State-level language.

b) In this regard, it is recommended that:

- Any measurement/ monitoring system must guarantee that there is sufficient server capacity and the service does not act as a bottleneck, thereby distorting results. A potential solution to this is the implementation of an access control system where only a specific number of users can measure there results at a given time.[3]
- As detailed in our response to Question 7, with respect to measurements collected from end-users factors like cross-traffic, measurement interface (fixed/wireless), firewalls, client operating system and hardware can influence measurement results.[4] These factors must be accounted for while analysing measurement data collected from end-users. The analysis of such data should ideally be done by field experts and TRAI should consider outsourcing such tasks in a manner similar to Brazil's Regulatory Authority ANATEL (Please see Table in Response to **Q7**).

- In a software based measurement system where user participation is required, there must be due consideration for the creation of a user-friendly system, which is not overtly complex and off putting for users. To this end an alternative approach is the adoption of hardware based measurement mechanisms which can monitor QoS measurements with the help of a probe which eliminates the

[3]BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.
[4]Net Neutrality Measurements: Regulatory Use Case and Problem Statement draft-nieminen-ippm-nn-measurements-00.txt, K. Nieminen, Internet Engineering Task Force, February 2017, https://tools.ietf.org/html/draft-nieminen-ippm-nn-measurements-00#page-4

requirement of the end-users. However, such systems are more expensive[5] and thus a careful economic impact assessment of such a regulatory scheme must be done.

- Another challenge which TRAI must address pertaining to the monitoring of QoS measurements and consequent TMP detection is regarding the point of the digital delivery chain where TMP is being deployed. With respect to this regulatory authorities such as Ofcom have explored ideas of extensive network tomography[6]where different detection tools are used and the resultant data collected requires analysis. Without this ability to pinpoint the TMP it can be difficult to ascertain which party has deployed TMP in question. Therefore, TRAI must also evaluate a cost-benefit analysis of implementing a detection system which extends only up the ISP leg or should they also seek to monitor potential TMPs being put in place beyond the ISP leg.

- As has been discussed in TRAI's consultation paper, caution must be exercised with respect to the considering the implementation of intrusive mechanisms like Deep Packet Information which compromises privacy.

c) Please refer to our response to Question 7. Due regard must be paid to utilisation of cited open source measurement tools. TRAI should also consider developing appropriate technologies with the contribution of local technical field experts and should assess the possibility of inviting global industry experts to discussions.

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

Response

Considering the experience of the Indian MAG, BARC India and Brazil's CGI.br, the following recommendations accrue -

- **Composition:** The collaborative body should include technical, legal and policy expertise, and be composed of:
    - Corporates that provide services over the internet – such as providers of video and other content, intermediaries, e-commerce companies and social network websites as well as industry bodies that represent them.
    - Academia – representatives from universities that specialize in technology, law and policy as well as other organizations engaged in academic research.
    - Civil society organizations – Not-for-profit organizations that have a net neutrality mandate and represent views and interests of citizens.
    - Government representatives – Representatives from TRAI, Department of Telecommunications, DEITy and any other relevant Department or Ministry.

[5] BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.

[6] A Study of Traffic Management Detection Methods & Tools, Prepared for Ofcom under MC 316, Predictable Network Solutions Limited, June 2015.

- Network engineers from TSPs and independent experts.

- **Transparency:** The frequency, agenda and post-meeting transcript as well as recommendations etc. should be subject to transparency stipulations and be available for access on the internet for public scrutiny.
- **Clear Functions:** The Terms of Reference or functions of the group should be clear and specific, and not general in nature. Possible functions for consideration are as follows –
    - **Monitoring:** The collaborative body should identify third-party partners, and coordinate and supervise TMP monitoring efforts with third-parties as outlined in Question 11 (c).
    - **Criteria and Ratings:** The collaborative body should determine and publish indicators for monitoring compliance with net neutrality. Based on the said indicators the body should publish 'ratings' to acknowledge adherence and identify non-compliance. This may include grievance redressal, results of monitoring by third party and the regulator, and verified data from service providers, experts etc. This will enable consumers to take an informed decision while choosing service providers and assert institutional pressure to avoid violations.
    - **Recommendations:** The collaborative body can recommend review of the net neutrality framework before the set date of revision in case demonstrable technological, regulatory or legal developments necessitate the same. The body can also recommend a framework for consultations during the ordinary review of net neutrality norms.
- **Review:** At the time of ordinary review of regulations as set forth under Question 13, the collaborative group's functioning and efficacy should also be reviewed. Issues discovered in the review should be suitably redressed.

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?

Response

- Any policy/regulations must contain a sunset clause which mandates the review of such policy/regulation every two years. A committee consisting of all major stakeholders (as defined under answer to question 10) and experts can also recommend revisions. It also must be ensured that the framework introduced after such revision must also contain an appropriate sunset clause to maintain its efficacy.

Q.14 The quality of Internet experienced by a user may also be impacted by factors such asthe type of device, browser, operating system being used. How should these aspects beconsidered in the NN context? Please explain with reasons.

Response

- *Not relevant for current consultation and should not be regulated differently at present.*

<u>Part II: Explanatory Memorandum</u>

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

Response

The following factors may be taken into account to contextualize a non-discriminatory rule to preserve net neutrality:

- Keeping the existing realities of a jurisdiction like India in mind, where penetration and speeds are low,it may not be possible to provide broadband on a best efforts basis without compromising efficient use of our limited resources.
- The factor that broadband demand is currently driven by video and other lag-sensitive services in Asia and the world, must be considered while determining a net neutrality framework. At the same time, leeway must be made for changing demand patterns and internet based innovations which may not be driven a video-led demand for broadband in the future.
- Thus, some measure of differentiation rather than discrimination should be allowed. It Is equally important to keep any net neutrality framework flexible to respond to changing realities. For example, when broadband connectivity and demand become ubiquitous in the future, or innovations in the network or of services change demand and supply patterns.

In this context, a non-discrimination rule must also reflect the multi-disciplinary aspect of net neutrality which considers technology, economics and legal tenets, as follows:

- In terms of network***technology***, traffic management for quality of service may be deployed on two types of occasions –
    - The *first* where there is a necessity, such as if the network is congested that reduces the quality for all users in that network or other exigencies, when there is a regular surge in traffic such as during peak times that reduces the quality of lag and time sensitive services such as VoIP, real-time gaming and video streaming. During these times some traffic may be throttled and others may be prioritized to ensure better quality of service till such time the network is capable of providing quality service on a best efforts basis.
    - The *second* is when there is a deliberate control of the network through traffic management for reasons other than necessity. Such reasons usually involve commercial considerations such as tie-ups with service providers to provide a 'fast-lane' or prioritize bundled services, reduce competition for ISPs that also provide over-the-top services or for smaller ISPs that do not have the bandwidth to support all services and prioritize providers based on commercial arrangements.

  While the former is unavoidable without compromising quality of service, the latter compromises net neutrality without necessarily improving the overall quality for all consumers. In fact, it may lead to detrimental impact on both consumers that do not use the services prioritized or throttled in furtherance of commercial arrangements as well as new entrants that increase competition in the market.

- In terms of the ***economics*** of providing internet services, it must be considered that proliferation of broadband in India is still in its nascent stage and depends heavily on private sector investment. More specifically, the private sector's investment in developing telecom infrastructure in India outdoes the government expenditure by a huge margin. Illustratively, between 2015-16 and 2016-17, the total amount of funds disbursed to States under USOF funded schemes stood at INR 6,671.44 Crore[7]. On the other hand, in 2014-15 alone, private telecom service providers invested INR 4,31,597 crore in fixed assets and INR 91,373 crore in capital works[8]. With average revenue per unit falling sharply in the last few quarters, the losses incurred by TSPs is piling up, thereby making the present situation even more critical. At the same time network efficiency, can increase with increasing competition. Thus, increasing competitiveness is also intrinsically important for protecting the goals of net neutrality by ensuring adequate growth in the network.In this regard, the concerns of small ISPs should be considered and suitable incentives may be provided through tax breaks, mechanisms like local loop unbundling etc.
- To determine the difference between discrimination and differentiation due consideration may be given to the ***legal principle*** of equality enshrined as a fundamental right under the Constitution of India. Specifically, the notion of equality has been derived from Preamble of the Indian Constitution, which guarantees equality of status and opportunity, and from Article 14 of the Constitution which prohibits discrimination on grounds such as religion, race, caste, sex. Nevertheless, the concept of equality does not provide that persons should be treated alike in all situations, irrespective of their ability or capacity. In fact, it does not mandate equal treatment when there are unequal circumstances or among unequal persons. The Supreme Court of India in Satish Chandra v. Union Of India[9] declared that the guiding principle of the article is that all persons and things similar circumstanced shall be treated alike both in respect of privilege conferred and liabilities imposed. Thus, forbidding discrimination between person who are substantially in similar circumstances. However, it does not forbid different treatment of the unequal's. Illustratively, the apex court in M.G. Badappanavar v. State of Karnataka[10]stated that any treatment of equals unequally or unequal's as equal is a violation of the basic structure of the Constitution. The rule rather is that there is equality only among equals and to equate unequal's is to perpetuate inequality.

With regard to the contextual needs of India and the relevance of technological, economic and legal considerations, it is recommended that the following factors qualify a non-discrimination rule aimed at preserving network neutrality as far as possible:

[7] Ministry of Communication's response to Starred Question no. 18 in Lok Sabha, dated November 16, 2016. Available at - http://164.100.47.190/loksabhaquestions/annex/10/AS18.pdf
[8] Ministry of Communication's response to Unstarred Question no. 564 in Lok Sabha, dated July 20, 2016. Available at - http://164.100.47.190/loksabhaquestions/annex/9/AU564.pdf
[9] Satish Chandra Anand v. Union of India, 1953 AIR 250
[10] M.G. Badappanavar. v. State Of Karnataka, 2000 Supp (5) SCR 302

- **Like traffic be treated alike. Only different types of traffic may be treated differently.** i.e. it should be service provider and origin/destination agnostic. For example, all service providers of the same type, such as video streaming or VoIP, may be prioritized when there is congestion. Emergency services may be of different varieties such as tele-medicine, VoIP calls to police forces etc. however they may be treated as a single class of emergency services and notified as such.
- **Any discrimination or differentiation of traffic be conducted out of necessity and not commercial considerations and should not be anti-competitive**. For example, differentiation of traffic is acceptable in exigencies and during peak hours if there is congestion but not for commercial considerations such as an agreement between content providers and TSPs. Further, packets that are not time and lag sensitive, such as emails, should not face any discrimination in the network, whereas other services such as video and VoIP be prioritized when the necessity arises.
- To ensure that differentiation of traffic is not done without necessity it should always be **limited in time and the criterion of necessity be provable through empirical data**.
- Any stipulation made in this respect, irrespective of whether these recommendations are considered, should be **flexible and subject to regular review** and updated based on stakeholder feedback to ensure that such stipulations keep pace with change in technology. For example, when the broadband infrastructure is robust enough to support bandwidth demand, there may not be any need for traffic management.

It is further recommended that:

- TRAI study and conduct a consultation to determine incentives forcertain stakeholders, such as small ISPs,beyond the extant framework. The goal of such an exercise is to promote competition and innovation and deter any circumvention ofthe goals of net neutrality. For example, without adequate competition among TSPs there is a danger that incumbent internet providers may circumvent necessary investment for expanding the network infrastructure by relying excessively on traffic management practices to handle congestion.

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

(a) Other jurisdictions do not necessarily define 'the internet' or related terms in their net neutrality framework. However, definitions that have been adopted are of two kinds-

i. **Technical** – For example, in Netherlands the Telecommunications Act, 1998 defines '***Public Electronic Communications Network'***, through which internet access services as – "*an electronic communications network used wholly or mainly for the provisions of publicly available electronics communication service, including a network for broadcasting programmes, insofar as this is done for the public"*; wherein ***electronic communications service*** is defined as – *"a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals via electronic communications network, including telecommunications services and transmission services in the networks used for broadcasting, but excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services. It does not include information society services, as defined in Article 1 of the notification directive, which do not consist wholly or mainly in the conveyance of signals via electronic communications networks*."

ii. **Descriptive** – For example, the Brazilian *Marco Civil da Internet* defines **internet** as –"*the system consisting of the set of logical protocols, structured on a global scale for public and unrestricted use, in order to enable communication of data between terminals, through different networks."*

- It is recommended that the definition of internet or internet service be kept inclusive and should include certain characteristics, as follows:
  - It is public in nature;
  - It does not include specialized services.

Regarding the exclusion of specialized services from its scope, the following factors may be considered:

- There is a need for differentiating between public internet services and specialized services, by keeping the latter out of the purview of net neutrality stipulations. The phrase 'specialized services should be defined narrowly. For example, EU's Regulation2015/2120 defines specialized services as "*services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality.*"
- Exemptions for specialized services should also be qualified. For example, EU's Regulation 2015/2120 subjects specialized services to the following conditions –
  - the network capacity is sufficient to provide the specialized service in addition to any Internet Access Service (IAS) provided;
  - specialized services are not usable or offered as a replacement for IAS;
  - specialized services are not to the detriment of the availability or general quality of the IAS for end-users.
- However, if specialized services cause network congestion over public internet then the net neutrality framework should apply. For example, as laid down by the BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, specialized services

should not be used to circumvent traffic management measures applicable to internet access services.

- There should not be an assumption that Internet of Things(IoT)or any other service is a specialized service as it may, at least partially, be offered over the internet. Further consultations may be conducted to ascertain an appropriate framework for future technologies like IoT.

It is recommended:

- Establish threshold QoS standards for public internet that should not be violated in providing for specialized services.
- Specialized services should be defined narrowly and network utilization by TSPs of specialized services vis-à-vis public internet should be monitored.
- No specific service or conception should be included in the exception such as Internet of Things as it may be provided over the internet or through a specialized service.

(b) Content Delivery Networks (Content Distribution Networks) aid in timely delivery of content to the consumer by bringing such content geographically closer to the user. It enables the delivery of content, when requested for by the consumer, from a local server operated by the CDN provider, rather than a remote internet server situated at a distance. As the information is not delivered over the internet core, there is less traffic congestion and the quality of services is higher, thereby reducing the need for TMPs.

It is recommended:

- CDNs enhance efficiency and quality and, therefore, should be encouraged. A framework should be established for transparency in the deployment of such technologies and arrangements. This may be subject to further consultation by TRAI.

With regard to direct interconnection arrangements, it must be kept in mind that the internet was designed to be connected from end-to-end wherein any point in the network can reach any other point in the network. While this is not true in practice (for example, firewalls prevent end-to-end connectivity), the theoretical value of the connection is maximised when the network can reach, and be reached by, all other connected networks.[11] In practice, TSPs achieve maximum connectivity possible on a best efforts basis that is necessitated and guided by the market and carried out based on interconnection or peering arrangements with other service providers. Being a market-based tool to ensure greater connectivity that benefits all relevant stakeholders, it is best if interconnection is left to the market. In any case, interconnection of any kind – whether between two TSPs or between a TSP and a content service provider, should not be prohibited, for example as done by NIXI for interconnection with content service providers.

Thus, it is recommended:

[11] Geoff Huston, "On the Internet Everyone Else is Connected to Everyone Else – Right?", APNIC Blog, 22 Feb. 2016. https://labs.apnic.net/?p=779

- Interconnection is beneficial for all stakeholders and should be left to the market rather than regulation.
- Under no circumstances should interconnection/peering be prohibited, as done by NIXI.

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
TMPs are acceptable as short-term solution to congestion and other exigencies but should not be regular and for commercial purpose (optimization). A list can be in the form of examples to show difference between reasonable and prohibited TMPs. It is recommended that:

- There should be a hybrid approach with a broad stipulation on reasonable TMPs and a narrow approach prohibiting some kinds of TMPs.
- TMPs refer to Reasonable Network Management practices which may be in the form of throttling or prioritization.
- It should be application agnostic.
- Unreasonable TMPs include commercial arrangements, anti-competitive practices and arrangements that violate application-agnosticism.
- Blocking should only be allowed for illegal activities as detailed in our response to Question 6.

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

Response
It is recommended that:

- Reasonable TMPs should necessarily be application agnostic.
- It may be useful to consider user preferences. However, there are no ready examples of enabling a consumer choice based model. Thus, the TRAI should hold a consultation to determine the same.

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]***

Response

- This requires further study and should be subject to future notification.

Q.6 Should the following be treated as exceptions to any regulation on TMPs? *[See Chapter3]*
(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
Generally, any exception to TMPs or classification as reasonable TMP should only be done through a lawful order given by an appropriate authority or competent court of law. Further, the provision allowing for exception in the net neutrality framework should include qualifications. Illustratively, Article 9 of the Brazilian *Marco Civil Da Internet* exemptsessential technical requirements and emergency service and mandates the responsible entity to –

• Abstain from causing any damage to the user;
• Act with proportionality and transparency;
• Provide users, in advance, with descriptive information on its traffic management and mitigation practices, including network security measures.
• Provide services on non-discriminatory commercial terms and refrain from anti-competitive practices.

Thus, in the case of the suggested exception, the following recommendations may be considered:

- The resultant network neutrality stipulations should allow emergency situations and services to be considered a reasonable TMP. However, it should also be specified in the relevant provision that the service so exempted must be mandated through a lawful order given by an appropriate authority or competent court of law and only after defining it narrowly. Further, the provision so contained in a net neutrality instrument should also be defined narrowly,considering the following factors:
    - Such emergency services should be caused by exigencies which may be natural such as earthquakes, wherein relief services may be prioritized, or man-made such as spread of malware.
    - It is critical that such an exception should not be used to block or throttle internet services for case that may be mandated by an appropriate order, but are not an emergency. For example, mobile internet was blocked for four hours across Gujarat in

February 2016 to prevent cheating in a state entrance exam.[12]This should not qualify as an emergency service under the net neutrality framework.

- Considering the nature of emergency situations *ex post facto* orders may be considered lawful.

- Unlawful content may be blocked only if mandated through a lawful order given by an appropriate authority or competent court of law, after defining it narrowly and only till such time the unlawful activity continues. For example, if a url/website is blocked for obscene content, it should be done only through an executive or court order and only till such time the objectionable content is available on it.
- It is essential to consider maintenance of security and integrity of the network as a reasonable TMP. However, the TMP must be proportionate to the threat and should only continue for the time-period necessary. Further, the instances of using TMPs for maintenance should be documented within a reasonable period of time and should be made available for regulatory/ public scrutiny as appropriate.
- If other services are notified as exceptions in public interest, since the phrase 'public interest' does not have an overarching definition, it should be done only on the basis of a defined category of services which may include providing essential welfare services such as transfer of subsidies. However, other initiatives by the Government that may benefit the public but is in economic competition with the private sector should not be exempted under the TMP framework.
- There should be no generic provision to allow 'any other services' for exemption.

Q.7 How should the following practices be defined and what are the tests, thresholds andtechnical 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
It is recommended that the following aspects be considered while defining blocking and differential/preferential treatment:

- Blocking refers to the practice of obstructing access to one or more service(s) of one or more consumer(s) by using traffic management practices or other means. Blocking should only be allowed in furtherance of a lawful order such as by an appropriate authority or by a competent court of law.
- Differential/ Preferential treatment includes throttling and prioritization wherein one or more service(s) is made less/more accessible in comparison to other services by reducing/ improving

[12]Freedom House: Freedom on the Net 2016 - India, November 2016, https://freedomhouse.org/sites/default/files/FOTN%202016%20India.pdf

the quality of service or by other traffic management practices and is only reasonable if non-discriminatory as given in our response to Question 1.

With regard to tests and technical tools to detect deployment of TMPS, the regulatory authorities must ideally know at what point along the digital path the concerned TMP is being deployed, to effectively identify the party responsible for the same. However, no studies on existing deployment of TMPs in India are available. Therefore, further development is required to formulate a broad TMP detection framework.

Illustratively, Ofcom, the United Kingdom's regulatory authority released an extensive report in 2015, of various widely utilised Traffic Management Detection tools, which detect particular kinds of TMPs. The study however concluded that there remain gaps, in the extant tools to detect TMPs at specific points along the digital delivery chain and called for the same to be studied.[13] The study also stresses on the development of a detection system which is scalable and does not require excessive implementation costs or is a burden on the overall network's performance.[14]
In the interim, before such a study is conducted and relevant monitoring tools are determined or createdcertain major open source and privately development measurement tools may be utilized, for example:

Sl. No.	Tool	System and Utilisation
1.	**SamKnows**	It is a proprietary framework with various tests measuring: • Video Streaming • Speed • Low Level Measurements including latency, packet loss and DNS • Web Browsing Measurements • VoIP Measurements Over 30 regulatory authorities collaborate with SamKnows.[15]
2.	**Electronic Frontier Foundation (EFF)**	• EFF has released Version Zero of Switzerland, an ISP testing software. Switzerland uses a semi-P2P, server-and-many-clients architecture to detect modified or spoofed traffic between multiple clients. • The Test Your ISP project previously released a much simpler piece of software called pcapdiff. Pcapdiff is a simple command line tool that lets you compare "pcap" packet captures from either end of an Internet communication; it reports when packets are dropped and spoofed between the endpoints ("pcap" packet captures can be recorded with standard packet sniffing tools like tcpdump and wireshark).

[13] A Study of Traffic Management Detection Methods & Tools, Prepared for Ofcom under MC 316, Predictable Network Solutions Limited, June 2015.
[14] Ibid.
[15] *The SamKnows internet measurement platform is actively testing in more than 30 countries on behalf of telecoms regulators*, Sam Knows, https://www.samknows.com/regulators

3.	**Glasnost**	• Aims to determine whether an individual user's traffic is being differentiated based on application. It does this by comparing the successive maximum throughputs experienced by two flows. • Used to develop aspects of Hungarian Measurement Tool • Endorsed by BEREC to evaluate degradation of performance of individual applications.[16]
4.	**Broadband Internet Service Mark (BISmark)**	• The BISmark is a research project and a collaboration effort between Georgia Tech, Princeton University and M-Lab, created to develop an open platform for home broadband internet research. BISmark research is centered but not limited to home network performance measurement (benchmarking). Volunteers can use BISmark to measure the performance of their ISP, visualize and monitor traffic patterns using their devices inside their home network.
5.	**MLab**	• M-Lab hosts a number of measurement tests ranging from network speed and latency to blocking and throttling • They host tests including Glasnost and BISmark. • Attempts to comprehensively measure all portions of QoS through a diverse range of tests
6.	**SpeedTest.Net developed by Ookla[17]**	• Open Source speed and broadband testing platform. Globally recognised as an industry leader. • Used as point of reference to develop aspects of Hungarian Measurement
7.	**Tools analysed by Ofcom 2015 Report**	a) **NetPolice**: aims to detect content- and routing-based differentiations in backbone (as opposed to access) ISPs. It does this by selecting paths between different access ISPs that share a common backbone ISP, and using ICMP to detect packet loss locations. b) **NANO:** aims to detect whether an ISP causes performance degradation for a service when compared to performance for the same service through other ISPs. It does this by collecting observations of both packet-level performance data and local conditions and by applying stratification and correlation to infer causality. c) **DiffProbe:** aims to detect whether an access ISP is deploying certain differential TM techniques to discriminate against some of its customers' flows. It does this by comparing the delays and packet losses experienced by two flows when the access link is saturated. d) **ShaperProbe**: tries to establish whether a token bucket shaper is being applied to a user's traffic. It does this by sending increasing bursts of maximum-sized packets, looking for a point at which the packet rate

[16] BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.
[17] Speedtest: The Global Standard in Internet Metrics, http://www.speedtest.net/

		measured at the receiver drops off. e) **ChkDiff**: tries to discern whether traffic is being differentiated on the basis of application. Rather than testing for the presence of a particular TM method, this approach simply asks whether any differentiation is observable, using the performance of the whole of the user's traffic as the baseline.

The efforts made in various jurisdictions/organisations to monitor the detection of unreasonable traffic management/ shaping practices are enumerated in the following table:

Serial No.	Jurisdiction/ Organisation	Type of TMP Detection Framework Adopted or Recommended
1.	**United Kingdom**	Ofcom works with SamKnows and has developed its own application, to measure mobile and broadband connections.[18]
2.	**France**	Has developed its measurement tool after prolonged stakeholder consultation process designed by a technical committee headed by their regulatory authority, in concert with affected TSPs, consumer associations and independent technical experts[19]
3.	**Croatia**	National Regulatory Authority has developed its measurement system, which was endorsed by the ITU. Results from the measurement tool can be used as evidence in customer complaint cases.[20]
4.	**Hungary**	Developed its own software and hardware measurement system. Uses elements of SpeedTest technology developed using elements of Ookla and Glasnost measurement tools.[21]
5.	**Singapore**	Works with SamKnows[22] to measure the QoS Practices of ISPs and their compliance with quarterly disclosures made to the regulatory authority. Non-compliance with disclosure requirements result in hefty fines for each violation[23]. All disclosures made to the Regulatory Authority are made publicly available.

[18]Ofcom broadband and mobile checker app, Ofcom, December 2016, https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/advice/ofcom-checker

[19]http://www.arcep.fr/index.php?id=8571&no_cache=1&tx_gsactualite_pi1%5Buid%5D=1744&L=1&cHash=211a5f1fbab796956d31ae8f17f13e95

[20]*Hakometar*,Hakom, (Croatian Regulatory Authority), https://translate.google.co.in/translate?hl=en&sl=hr&u=https://www.hakom.hr/default.aspx%3Fid%3D1144&prev=search,

[21]Testing the quality of Internet services in Hungary : The software and hardware based public measurement system of NMHH, Zsolt TORMA, ITU, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Broadband%20Mapping/1.%20Zolts-Torma-%20Hungary-Warsaw_final.pdf

[22]*The SamKnows internet measurement platform is actively testing in more than 30 countries on behalf of telecoms regulators*, Sam Knows, https://www.samknows.com/regulators

[23]Quality of Service Reports, INFOCOMM Media Development Authority, March, 2017, https://www.imda.gov.sg/regulations-licensing-and-consultations/licensing/licences/licence-for-the-sale-of-telecommunication-equipment/compliance-to-imda-standards/quality-of-service/quality-of-service-reports; Quality of Service, INFOCOMM Media Development Authority, December 2016, https://www.imda.gov.sg/regulations-

6.	**Brazil**	Regulatory authority ANATEL, has worked in collaboration with SamKnows' measurement tools and the QoS measurement is outsourced through a competitive bidding process. The winner of the bid collaborates with SamKnows.[24]
7.	**Serbia**	Regulatory Authority has developed its own system called Ratel NetTest recommended by ITU.
8.	**Austria**	Regulator developed own measurement system called RTR NetTest[25]
9.	**ITU**	Endorses systems such as RTR NetTest developed by Austria, SamKnows, Croatian regulatory tool i.e. HakoMetar,[26] and Serbia's measurement system Ratel NetTest[27]
10.	**BEREC**	Although recommends developing standardised measurement systems, the Guidelines mention that tools such as Glasnost can be used to evaluate degradation of the performance of individual applications.[28]

There is a need to first select objective measurement metrics. For example, the French measurement system, developed after intensive consultation with relevant stakeholders,[29] has four evaluative technical indicators - upload speed, download speed, latency and packet loss. It also has factors which account for specific types of online usage such as web browsing, video streaming and P2P downloads. BEREC, while mentioning technical parameters, listed upload and download speed, delay, jitter, and packet loss ratio.[30]They also place a reliance to determine technical parameters on regional bodies and international standard setting organisation such as also provide us with two key takeaways the Internet Engineering Task Force.[31] The ITU has also endorsed metrics for QoS evaluation that include:

- *"Speed (refers to all service functions),*
- *Accuracy (e.g., speech quality, call success ratio, bill correctness, etc.),*
- *Availability (e.g., coverage, service availability, etc.),*

licensing-and-consultations/licensing/licences/licence-for-the-sale-of-telecommunication-equipment/compliance-to-imda-standards/quality-of-service

[24]*Mobile Internet Services in India Quality of Service*, Published by Communication Unity and Trust Society & Indian Institute of Technology Delhi, IIT Delhi, July 2016, http://www.iitd.ac.in/research/IITD/1615_QoS_Report_CUTS_IIT.pdf

[25]RTR-NetTest, https://www.netztest.at/en/

[26]*Hakometar*,Hakom, (Croatian Regulatory Authority), https://translate.google.co.in/translate?hl=en&sl=hr&u=https://www.hakom.hr/default.aspx%3Fid%3D1144&prev=search,

[27] Ratel Net-Test, Developed by Regulatory Agency for Electronic Communications and Postal Services (RATEL), Serbia, https://www.nettest.ratel.rs/en/about

[28]BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.

[29]ARCEP publishes its quality of service scoreboard for fixed internet access, and begins a period of assessment and enhancement of its system, Arcep, May 2015, http://www.arcep.fr/index.php?id=8571&L=1&tx_gsactualite_pi1%5Buid%5D=1701&tx_gsactualite_pi1%5Banne e%5D=&tx_gsactualite_pi1%5Btheme%5D=&tx_gsactualite_pi1%5Bmotscle%5D=&tx_gsactualite_pi1%5BbackI D%5D=26&cHash=f558832b5af1b8e505a77860f9d555f5

[30] BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.

[31] BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.

- *Reliability (e.g., dropped calls ratio, number of billing complaints, etc.),*
- *Security (e.g., fraud prevention),*
- *Simplicity (e.g., easy of software updates, easy of contract termination,*
- *Flexibility (e.g., easy of change in contract, availability of different billing methods such as online billing, etc.).”*[32]

Additionally, TRAI must also take into consideration that software based measurements, can be influenced by extraneous factors such as firewalls, cross-traffic, system hardware and other technical considerations (further elaborated in **Q11**).[33] However, given the vastness of the infrastructure, TRAI must conduct a consultation to evaluate the economic feasibility of hardware based monitoring/ measurement systems.

In this context, we must note that there have been efforts within India by universities such as the Indian Institute of Technology (‘IIT’), Delhi to develop indigenous QoS measuring systems.[34] We believe this is an important step which shall aid in TRAI’s efforts to detect and aptly regulate unreasonable traffic management/ traffic shaping practices. These initiatives can learn from ventures such as Broadband Internet Service mark (BISmark), launched by Georgia Tech for (broadband) internet measurement which has been briefly discussed in the above.[35]

Based on our findings, we recommend the following initial regulatory efforts with regard to TMP detection:

- Before an indigenous TMP detection system is developed, TRAI should seek to identify and authorize testing tools to facilitate official monitoring of unreasonable TMPs. Tools offered by open systems such as Ookla, Glasnost and Mlab and private entities such as SamKnows, can be useful for this initiative.
- Simultaneously, there must be a comprehensive stakeholder consultation by TRAI with ISPs, consumers, public policy entities, academic and industry experts, etc. to collectively determine and standardize an appropriate TMP detection regime, including:
    - To develop detection/ measurement parameters such as download speed, upload speed, jitters, packet loss ratio, latency, etc. Technical recommendations, standards, technical specifications and guidelines from international bodies such as the ITU, International Organisation for Standardisation (‘ISO’) and the International

[32] Milan Jankovic, *Regulatory challenges related to the Quality of Service and Experience*, International Regulatory Conference for Europe Regulating Electronic Communication Market 26-27 September 2016, ITU, http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Regulatory%20Conference/MILAN%20JANKOVIC.pdf

[33] Net Neutrality Measurements: Regulatory Use Case and Problem Statement draft-nieminen-ippm-nn-measurements-00.txt, K. Nieminen, Internet Engineering Task Force, February 2017, https://tools.ietf.org/html/draft-nieminen-ippm-nn-measurements-00#page-4

[34] *Mobile Internet Services in India Quality of Service*, Published by Communication Unity and Trust Society & Indian Institute of Technology Delhi, IIT Delhi, July 2016, http://www.iitd.ac.in/research/IITD/1615_QoS_Report_CUTS_IIT.pdf

[35] Ibid.

Electrotechnical Commission ('IEC') can be used as a point of reference.[36] The final decision with respect technical criteria should be made after appropriate consultation with technical experts.

- To develop an official measurement/ monitoring system which fits India's internet ecosystem, appropriate consideration must be given to parties who have relevant experience in the development of such systems, such as IIT Delhi. Moreover, TRAI may analyse national measurement systems/ applications by other jurisdictions such as Hungary, France, Croatia, Austria, Serbia and the UK and assess the feasibility of adopting their detection tools to India's net neutrality regime.
- To determine if a software based monitoring mechanism will suffice or if a hardware based mechanism is required as well.

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 publishsuch information?

Response

Transparency is an integral aspect of net neutrality. Thus, disclosures to the public, potential consumers and existing consumers ensure that the consumer is aware enabling them to make an informed decision while choosing service providers and the kind of service they can expect to be provided. At the same time, if the disclosure to consumers and the public are heavily technical and complicated it is likely that the consumer/ public will not benefit from the disclosure for the simple reason that only those who have the technical knowledge and training can understand it. Thus, disclosures that are necessary to determine the practices of TSPs, but are more technical in nature should be more to a specialized body that can determine its import. At the same time, such disclosure must be periodical to ensure that any updates are also communicated to the public and triggered by an offer or an agreement to buy the services such that the consumer can make an informed decision before purchasing the service. In this context we may consider the approach taken in Singapore where all disclosures made by ISPs to the Singapore regulatory authority are made public which helps users make informed choices on the plan they want to opt for. This practice creates an opportunity for users to switch ISPs and thus due to competition between industry players the market place works to limit unreasonable TMP deployment. The ITU also suggests that the regulator should keep a publicly available and updated database of prices,

[36]Milan Jankovic, *Regulatory challenges related to the Quality of Service and Experience*, International Regulatory Conference for EuropeRegulating Electronic Communication Market26-27 September 2016, ITU, http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Regulatory%20Conference/MILAN%20JANKOVIC.pdf

conditions of access and use (including limitations), and the quality of public communication networks and services.[37]

Therefore, it is recommended:

- A **mixed approach** be adopted wherein –
    - The consumer and public are kept informed of all the details required to make an informed decision such as QoS, expected speeds, contention ratio, traffic management practices etc. without compromising readability due to technical details.
    - The regulatory disclosure is more detailed in nature and contains technical information regarding frequency of congestion, reason for using traffic management, type of TMP used etc.

With regard to the trigger, mode and frequency for publishing such information, it is recommended:

- **Public** - The disclosure must be made to the public along with the display of the offered data plan and services. For example, the updated disclosure should be available at point of purchase, along with advertisements and along with any other communication to the public regarding data plans and other services. Additionally, all such disclosures should be made in at least two languages including English and the major regional/state-level language.
- **Consumer** – The consumer should be informed specifically every time there is an update in the practices of the TMP through the mode of communication opted for by the consumer (email, post, phone number etc.). Additionally, all such disclosures should be made in at least two languages including English and the major regional/state-level language.
- **Regulator** – The regulator should receive disclosures at the end of every month with a summary of the congestion experienced and TMP used by TSPs in that month. Further, the regulator will also be kept informed of any updates to the disclosures provided to the public and consumers. The information should be available for perusal by the public on the TRAI website. However, this does not include information that may compromise proprietary secrets or confidential information.

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

Response

The Information Disclosure Template is an important facet of disclosure for transparency in traffic management practiced by different ISPs. While the format suggested by TRAI is appropriate, there are omissions noticed that may lead to vague or partial communication of information, as follows:

[37]Milan Jankovic, Regulatory challenges related to the Quality of Service and Experience, International Regulatory Conference for Europe Regulating Electronic Communication Market 26-27 September 2016, ITU, http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Regulatory%20Conference/MILAN%20JANKOVIC.pdf

- Under 'Other Terms and Conditions' the download limit, upload limit, data usage caps and fair usage policies should all be mentioned separately to avoid confusion and for better consumer readability.
- Under 'Application Specific Traffic Management' ('Service Limitations and Traffic Management') there should be an additional parameter to disclose bandwidth throttling as follows – "*Are any services, content, applications or products always **throttled** on this plan?*"
- There should be an additional parameter for specifying traffic management practices for any other reason as follows – "*Are TMPs deployed for any other reason? Please specify the reason, the services affected and the type of TMP used (blocking, throttling, prioritization).*"
- There should be a glossary of terms listing out definitions of technical words (such as TMP, latency, blocking, throttling, prioritization etc.) at the end of the Template for the benefit of the consumer.

Comparatively, the Template is similar to UK's Free Internet Key Facts Indicators (KFI) (annexed), thus the same may be relied on to review the efficacy of implementation. The following points emerge from such an exercise –

Accessibility:

- The KFI information for different ISPs is available as a compilation on the website of The Broadband Stakeholder Group (BSG) - an advisory group on broadband that works with the UK Government.
- It was not readily accessible on the website of OFCOM – UK's communications regulator.
- It was not readily accessible from the websites of the companies. There was no standardized link to access it i.e. different ISPs locate it in different parts of their website (eg. legal or community). It is not displayed along with description of various broadband plans.
- Out of 14 ISPs listed, only 9 links directly go to a URL on traffic management practices or the KFI.

Quality of Disclosed Information:

- None of the KFIs have any indication of time and date or updates.
- Only 4 out of 14 KFIs deal with individual plans. Most of them list the product description required under the KFI as 'all mobile tariffs' or similar.
- There is no indication of whether the information provided in the KFI has been verified for example by a regulator or third-party auditor.
- A tabulated-format for disclosing peak time traffic management on specified services works well to disclose information by ISPs and to compare information so disclosed.

Based on the comparative analysis it is recommended:

- Clear ***accessibility*** requirements be set out. Specifically:
    - A separate template be made for each plan or cluster of similar plans but not of all or different types of plans (entry level, unlimited etc.).

- Each ISP should display the Template at point-of-sale and where the plans are displayed on its website rather than under other topics like legal, community etc.
- A complied list of Templates from different ISPs be made available on the TRAI website and website of any co-regulatory or other body so empowered linking the actual URL containing the Template rather than the website of the ISP.

- A clear ***timeline*** be set out for the publishing of templates, including:
  - An annual **date** when the availability and up-to-datedness of the Template can be ascertained. There should also be random checks to ensure the continued availability of Templates.
  - If they Template requires updating to reflect changes/additions in plans the same should be intimated to the TRAI or any other body set up for this purpose such that it may be verified and reflected in lists complied by TRAI or any other body empowered to do so.
  - The Template should include a date to reflect the date of the last update.
- The Template so displayed by ISPs should be subject to ***independent and regulatory audits****(see also response to Q.11)*, preferably both, and this information be displayed by ISPs on their Template, as follows:
  - The independent audit may be conducted by a designated organization empaneled for this purpose that has the capacity to verify based on empirical and statistical testing. This can be a civil society organizations, a technical institution such as an information technology university or a multi-stakeholder body.
  - The regulatory audit may be conducted based on information received by the empaneled agency or multiple agencies as well as based on information independently obtained by the regulator. This can be done by TRAI, a co-regulatory or other body set up empowered to do so or a combination of the two.
- It is recommended that a tabulated-format for publishing traffic management of specific services or type of trafficbe appended at the end of the Template, such as the one used in the KFI, with slight modifications as follows:

Sl. No.	**Traffic Type**	**Blocked**	**Slowed Down**	**Prioritized**	**Reason**(eg. peak time, congestion, emergency)
1.	Peer to peer				
2.	News				
3.	Browsing/email				
4.	VoIP (Voice over IP)				
5.	Gaming				
6.	Audio streaming				
7.	Video Streaming				
8.	Audio download				
9.	Video download				

10.	Other download (please specify)				
11.	Instant Messaging				
12.	Background/ Software Updates				
13.	Other (please specify)				

Q.10 What would be the most effective legal/policy instrument for implementing a NN framework 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
(a) The TRAI should be responsible for monitoring and supervision informed by the recommendations of a collaborative body.

(b) Different bodies are competent to determine different kinds of disputes and the penalties applicable have been provided for. Broadly, existing jurisdictions cater to two categories of disputes –

I. Consumer Disputes
II. Disputes between service providers

The following statutes contain relevant provisions –

- The Indian Telegraph Act, 1885
- The Consumer Protection Act, 1986
- The Telecom Regulatory Authority of India Act, 1997
- Competition Act, 2002

Further, the judiciary is a competent appellate body.

a. Indian Telegraph Act, 1885 –

Consumer Disputes: Section 7(b) of the Indian Telegraph Act, 1885 provides for arbitration in cases of dispute between a consumer and the telegraph authority. The provision reads –

***7B. Arbitration of disputes**.—(1) Except as otherwise expressly provided in this Act, if any dispute concerning any telegraph line, appliance or apparatus arises between the telegraph authority and the person for whose benefit the line, appliance or apparatus is, or has been provided, the dispute shall be determined by arbitration and shall, for the purposes of such determination, be*

referred to an arbitrator appointed by the Central Government either specially for the determination of that dispute or generally for the determination of disputes under this section.

b. Consumer Protection Act, 1986 –

Consumer Disputes: For a long time, consumer forums did not address telecom related consumer disputes based on an Order[38] of the Supreme Court of India, dated September 01, 2009, wherein a two judge bench held that since there is a special remedy available under Section 7B of the Telegraph Act, the remedy under the Consumer Protection Act is barred by implication.

However, in 2014, the Department of Telecommunication vide an office memorandum, clarified that consumer forums have the jurisdiction to adjudicate disputes between a consumer and a telecom service provider.

Additionally, in the recently introduced Consumer Protection Bill, 2015, which may replace the extant consumer protection statute, the definition of services under Clause 2(37) explicitly includes *'telecom'* as one of the services.

Thus, consumer forums can exercise jurisdiction and impose penalties in the following cases –

Disputing Parties	Original Jurisdiction	Appellate Jurisdiction
Consumer v. TSP	Upto INR 20 Lacs – District Consumer Forum	State Commission → NCDRC → Supreme Court of India
	>20 Lakh < 1 Crore – State Consumer Commission	NCDRC → Supreme Court of India
	>1 Crore – National Consumer Dispute Redressal Commission	Supreme Court of India

Further, as per Section 27 of the Consumer Protection Act, 1986, willful non-compliance of forum's order attracts imprisonment up to three years and monetary fine up to INR 10,000.

c. The Telecom Regulatory Authority of India Act, 1997 –

Consumer Disputes: The preamble to the TRAI Act includes protection of consumers as one of the purposes of the Act and the institutions created therein. Following provisions deal with protection of consumer interests in the Act –

- Section 11 lays down protection of consumer interest as one of the functions of TRAI.
- Section 14 provides for establishment of the Telecom Disputes Settlement and Appellate Tribunal which can inter-alia adjudicate any dispute between a service provider and a *group of consumers*.

[38] Civil Appeal No. 7687 of 2004

- Section 14A of the Act also empowers *'any person'* to make an application for adjudication of any dispute the tribunal is competent for.

As per the judgment of the Supreme Court of India in Cellular Operators Association of India v. Union of India, TDSAT is an expert body whose jurisdiction in telecom matters is wider than that of the Supreme Court of India itself. However, given that there is just one bench of the tribunal in India, it is logistically the most difficult to approach by consumers. Moreover, TDSAT is only empowered to adjudicate disputes between a service provider and a *group of consumers*. Thus, a single consumer cannot approach TDSAT.

Disputes between service providers: Any dispute arising between two telecom service providers or between the licensor and licensee falls in the jurisdiction of TDSAT which enjoys both, original as well as appellate jurisdiction. Section 14 of the TRAI Act, 1997 empowers TDSAT to adjudicate disputes between two TSPs or a licensor and licensee.

It is pertinent to mention that TRAI too has recommendatory powers under Section 11 of the TRAI Act, 1997 vide which it can recommend revocation of license for non-compliance of terms and conditions of a license. Additionally, TRAI has also been vested with anti-trust jurisdiction vide Section 11 (1) (iv) of the TRAI Act, 1997.

Thus, TDSAT exercises jurisdiction in the following cases –

Disputing Parties	Original Jurisdiction	Appellate Jurisdiction
TSP v. Group of Consumers	TDSAT	Supreme Court of India
Two or more TSPs	TDSAT	Supreme Court of India
Licensor and Licensee	TDSAT	Supreme Court of India

Further,Section 20 of the TRAI Act, 1997 provides for monetary fine up to INR 1 lakh on willful non-compliance of the orders of TDSAT. Subsequent contravention attracts fine of INR 2 lakh and continuing violation attract penalty at INR 2 lakh per day. Section 29 of the Act provides for identical punitive actions for willful non-compliance of TRAI's guidelines.

d. Competition Act, 2002 –

Consumer Disputes: Protection of consumer interests finds an express mention in the preamble to the Competition Act, 2002. Both, Competition Commission of India as well as the Competition Appellate Tribunal, as created under the Act have jurisdiction over telecom matters where anti-competitive practices or abuse of dominant position causes hardship to the consumer. This jurisdiction is not voided by the jurisdiction of the TRAI or the TDSAT, which deal with more technical matters. This was made clear in the order in the case of *Sonam Sharma and Apple Inc. USA, Apple India Pvt. Ltd., Vodafone Essar Limited and Bharat Airtel Limited[Case No. 24/2011]*[39]Here, the informant alleged anti-competitive

[39] Judgment of the Competition Commission of India, in the matter, dated 19.03.2013. Available at - http://www.cci.gov.in/sites/default/files/242011_0.pdf

agreements between Apple and the telecom providers, wherein iPhones were being sold locked to a network provider with special data plans which were priced differently than those for other phones. The informant accused the opposite parties of abuse of dominant position. One of the Opposite Parties, Vodafone, submitted that the CCI had no jurisdiction as this was a telecom issue especially that of tariffs, and TRAI and TDSAT would have jurisdiction. This was rejected by the Commission, which held that wherever and as far as anti-competitive practices are involved, it has.

Disputes between service providers: Being the competition regulator, the Competition Commission of India exercises general powers of maintaining sustainable competition and the telecom sector is no exception. Despite TDSAT being an expert body for adjudicating telecom disputes, the competition regulator's jurisdiction is saved in the first proviso to Section 14 of the TRAI Act, 1997. The ongoing dispute between Reliance Jio and Airtel is an example of TSPs being amenable to anti-trust jurisdiction.

Thus, CCI exercises jurisdiction in the following cases –

Disputing Parties	Original Jurisdiction	Appellate Jurisdiction
Consumer v. TSP	CCI	COMPAT → Supreme Court
Two or more TSPs	CCI	COMPAT → Supreme Court

Further, Section 42 of the Competition Act grants the commission, powers to levy fines or order imprisonment for non-compliance of its orders. Section 43A provides for levying of fine up to 1 percent of annual turnover for failing to furnish certain information in reference to combinations under S.6(2). CCI can pursue multiple remedies against anti-competitive practices even to the extent of dividing a dominant enterprise. The CCI has been given the power under section 19 of the Act to carry out inquiries into any alleged contravention of the provisions of section 3 and 4, which deal with anti-competitive agreements and abuse of dominant position respectively.

e. Jurisdiction of Judiciary –

The jurisdiction of superior courts in regulatory issues are well defined and unless otherwise provided, are limited to ascertainment of a substantial question of law or determining the legality of a decision.

While the TRAI and TDSAT are the most appropriate forums to adjudicate disputes, and impose penalties for net neutrality violations the only bench in existence is in Delhi. Further, the TDSAT is only empowered to hear a class of consumers and not an individual. Thus, it is recommended that:

- TRAI and TDSAT should be the appropriate forum for dispute settlement and imposition of penalties under the net neutrality framework. The penalty may be in the form of daily fines till the cessation of the violation. If the violation crosses a threshold then the case should be escalated to the Department of Telecommunications who can suspend or cancel the license of the incumbent. For example, the threshold may be three violations before escalating to the DoT or violations extending to more than 30 days cumulatively in a year.

- Considering the logistical and other limitations of the TRAI and TDSAT the jurisdiction of other appropriate forums, such as the Consumer Forum and Competition Commission, should not be ousted.

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

While there are several nuanced technological challenges which TRAI must addressed while developing a framework to monitor unreasonable traffic management/ traffic shaping practices, we shall highlight some broad concerns which require close attention.

a) Disclosures and Information from TSPs and associated challenges:

- The BEREC guidelines on the monitoring of internet access service in the context of net neutrality provides us with a key takeaway (as was highlighted in our response to Question 7) that it is imperative to have a standard/ officially accepted monitoring mechanism as, otherwise it leaves scope for ISPs to deny the veracity of results by questioning the legitimacy of the measurement tool.[40]

  Therefore, it is recommend that:
  - If TRAI adopts interim measures for TMP detection using open source measurement systems, they must clearly endorse the tools which are officially accepted as legitimate by way of notification.
  - Moreover, TRAI may be required to create a database where overall measurements are stored and analyse to determine the widespread TMP practices of ISPs. If TRAI chooses to publish "raw" data from any official measurement tool/ monitoring system, developed in the future, for the sake of transparency it must be ensured that privacy of users is not compromised.

- Regarding language of disclosure, as detailed in our response to Question 8, it is reiterated that:
  - The publication/ disclosure of TMP practices must not be buried within service agreements or in complex technical language. There must be easily traceable, and enumerated in comprehensible language. To this end, TRAI must explore if such disclosures of official TMP

[40]BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.

policy are published in multiple languages including English and the major regional/State-level language.

b) Collection of Information from users and associated challenges:
In this regard, it is recommended that:

- Any measurement/ monitoring system must guarantee that there is sufficient server capacity and the service does not act as a bottleneck, thereby distorting results. A potential solution to this is the implementation of an access control system where only a specific number of users can measure there results at a given time.[41]

- As detailed in our response to Question 7, with respect to measurements collected from end-users factors like cross-traffic, measurement interface (fixed/wireless), firewalls, client operating system and hardware can influence measurement results.[42] These factors must be accounted for while analysing measurement data collected from end-users. The analysis of such data should ideally be done by field experts and TRAI should consider outsourcing such tasks in a manner similar to Brazil's Regulatory Authority ANATEL (Please see Table in Response to **Q7**).

- In a software based measurement system where user participation is required, there must be due consideration for the creation of a user-friendly system, which is not overtly complex and off putting for users. To this end an alternative approach is the adoption of hardware based measurement mechanisms which can monitor QoS measurements with the help of a probe which eliminates the requirement of the end-users. However, such systems are more expensive[43] and thus a careful economic impact assessment of such a regulatory scheme must be done.

- Another challenge which TRAI must address pertaining to the monitoring of QoS measurements and consequent TMP detection is regarding the point of the digital delivery chain where TMP is being deployed. With respect to this regulatory authorities such as Ofcom have explored ideas of extensive network tomography[44]where different detection tools are used and the resultant data collected requires analysis. Without this ability to pinpoint the TMP it can be difficult to ascertain which party has deployed TMP in question. Therefore, TRAI must also evaluate a cost-benefit analysis of implementing a detection system which extends only up the ISP leg or should they also seek to monitor potential TMPs being put in place beyond the ISP leg.

[41]BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.
[42]Net Neutrality Measurements: Regulatory Use Case and Problem Statement draft-nieminen-ippm-nn-measurements-00.txt, K. Nieminen, Internet Engineering Task Force, February 2017, https://tools.ietf.org/html/draft-nieminen-ippm-nn-measurements-00#page-4
[43] BEREC, Monitoring quality of Internet access services in the context of net neutrality (update after public consultation, BoR (14) 117, September 2014.
[44]A Study of Traffic Management Detection Methods & Tools, Prepared for Ofcom under MC 316, Predictable Network Solutions Limited, June 2015.

- As has been discussed in TRAI's consultation paper, caution must be exercised with respect to the considering the implementation of intrusive mechanisms like Deep Packet Information which compromises privacy.

c) Collection of information from third parties and public domain

- Please refer to our response to Question 7. Due regard must be paid to utilisation of cited open source measurement tools. TRAI should also consider developing appropriate technologies with the contribution of local technical field experts and should assess the possibility of inviting global industry experts to discussions.

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

Yes, a collaborative group should be formed under the aegis of the Department of Telecommunications (DoT) or TRAI. The primary regulatory authority and final decision-maker should continue to be TRAI and the Department of Telecommunications, respectively.

India has supported the adoption of a multi-stakeholder model for internet governance issues such as the 'delineated-role' model[45] espoused in clause 35 of the Tunis Agenda for the Information Society, 2005[46]. An example of an existing Indian collaborative group in the field of Internet Governance is the Multi-stakeholder Advisory Group (MAG) for the India Internet Governance Forum:

[45] http://unctad.org/Sections/un_cstd/docs/WGEC_IndiaMission.pdf

[46] We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:

1. Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.
2. The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields.
3. Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role.
4. Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues.
5. International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

- The MAG was constituted in 2014 by the Department of Electronics and Information Technology (DEITy) and included representatives from the government, private sector, civil society, academia and technical experts.
- The terms of references were general in nature and included reviewing the global policy landscape, providing inputs and suggestions, serving as a platform for multi-disciplinary knowledge sharing and building consensus for inputs to the Inter-Ministerial Group for Internet Governance.
- The tenure was set for three years and the group was to meet every six months.[47]
- Significantly, the MAG was consulted by the DoT Net Neutrality Committee.
- However, it is uncertain how many meetings have taken place till date, and no transcripts of the meetings are accessible. Further, hitherto there is no notification regarding re-constitution of the group as its tenure ends in 2017.

In the past TRAI has recommended co-regulation in the broadcasting sector. Specifically, in its recommendations dated August 19, 2008, TRAI recommended self-regulation of the television rating agencies by an industry led body – Broadcast Audience Research Council. Under the recommended model, the government exercised oversight functions through its nominees in the industry body. Set up in 2015, BARC is an industry body that designed and commissioned, and supervises India's television audience measurement system, which is also owned by it. It includes representatives of private broadcasters, advertisement agencies, advertisers and the government (i.e. Doordarshan).

An example of a mature collaborative mechanism for internet governance is the Brazilian Internet Steering Committee (CGI.br),[48] established in 1995. The CGI.br was amended in 2003 with the objective of coordinating and integrating initiatives, and promoting technical research, innovation and diffusion of Internet. It consists of five stakeholder groups: the federal government, the corporate sector, civil society and experts (third sector), and the scientific and technological community, with set timelines for holding ordinary meetings and provisions for extraordinary meetings. Further, CGI.br publishes the working agenda before meetings and a transcript after meetings on every issue discussed. Notably, the Government has to consult the CGI.br regarding aspects of net neutrality along with the National Telecommunications Agency under the *Marco Civil Da Internet*[49]. Its other notable achievements include the creation of Principles of Governance and Use of Internet, a set of ten principles providing a guide for future decision making on Internet governance.[50]

Considering the experience of the Indian MAG, BARC India and Brazil's CGI.br, the following recommendations accrue -

- **Composition:** The collaborative body should include technical, legal and policy expertise, and be composed of:

[47] http://cis-india.org/internet-governance/blog/mag-order.pdf
[48] http://cgi.br
[49] Article 9, Brazilian Internet Bill of Rights, 2014
[50] http://cgi.br/principles/

- Corporates that provide services over the internet – such as providers of video and other content, intermediaries, e-commerce companies and social network websites as well as industry bodies that represent them.
- Academia – representatives from universities that specialize in technology, law and policy as well as other organizations engaged in academic research.
- Civil society organizations – Not-for-profit organizations that have a net neutrality mandate and represent views and interests of citizens.
- Government representatives – Representatives from TRAI, Department of Telecommunications, DEITy and any other relevant Department or Ministry.
- Network engineers from TSPs and independent experts.

- **Transparency:** The frequency, agenda and post-meeting transcript as well as recommendations etc. should be subject to transparency stipulations and be available for access on the internet for public scrutiny.
- **Clear Functions:** The Terms of Reference or functions of the group should be clear and specific, and not general in nature. Possible functions for consideration are as follows –
  - **Monitoring:** The collaborative body should identify third-party partners, and coordinate and supervise TMP monitoring efforts with third-parties as outlined in Question 11 (c).
  - **Criteria and Ratings:** The collaborative body should determine and publish indicators for monitoring compliance with net neutrality. Based on the said indicators the body should publish 'ratings' to acknowledge adherence and identify non-compliance. This may include grievance redressal, results of monitoring by third party and the regulator, and verified data from service providers, experts etc. This will enable consumers to take an informed decision while choosing service providers and assert institutional pressure to avoid violations.
  - **Recommendations:** The collaborative body can recommend review of the net neutrality framework before the set date of revision in case demonstrable technological, regulatory or legal developments necessitate the same. The body can also recommend a framework for consultations during the ordinary review of net neutrality norms.
- **Review:** At the time of ordinary review of regulations as set forth under Question 13, the collaborative group's functioning and efficacy should also be reviewed. Issues discovered in the review should be suitably redressed.

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

Expressly written regulations have the force of law and the backing of sanctions increases its efficacy to address the mischief they are intended to address. However, in order to maintain their efficacy, regulations, much like laws, must evolve organically. Given the lengthy procedure involved in their

amendment, regulations are marred by rigidity. This reduces their relevance, especially in regulating sectors like telecommunications and internet, which evolve at such breakneck pace.

On the contrary, while self-regulation is a more viable model, its lack of legal sanctions makes it prone to contraventions, especially when the contours of such policy change frequently.

Thus, to keep pace with evolving technology, it is important to maintain the flexibility of any proposed framework by mandating its periodic revision. To achieve this, any proposed regulation/policy framework should contain a 'sunset clause' which ensures that the framework is revised either after the passage of a stipulated period of time or on the occurrence of a trigger event. Sunset clauses are not new to telecommunication regulations in India. TRAI's Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 contains a sunset clause.

Clause 6 of the said regulation allows TRAI to review the regulations on the expiry of two years or on any other date as it deems fit. However, the clause uses the word 'may' which does not make the stipulated review mandatory. In the present case, frequent review of any suggested measure is imperative by the application of Moore's law on any technology intensive sector.

Thus, it is recommended:

- Any policy/regulations must contain a sunset clause which mandates the review of such policy/regulation every two years. A committee consisting of all major stakeholders (as defined under answer to question 10) and experts can also recommend revisions. It also must be ensured that the framework introduced after such revision must also contain an appropriate sunset clause to maintain its efficacy.

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

Response

- *Not relevant for current consultation and should not be regulated differently at present.*