Telecom Regulatory Authority of India

Consultation Paper
on
Net Neutrality

4th January 2017

Mahanagar Door Sanchar Bhawan,

J.L. Nehru Marg, (Old Minto Road)
New Delhi - 110002, India

Stakeholders are requested to send their written comments, preferably in electronic form, by 15th of February 2017 and counter-comments by 28th of February 2017 to Shri Asit Kadayan, Advisor (QoS) TRAI on the email address advqos@trai.gov.in. Comments and counter-comments will be posted on TRAI's website www.trai.gov.in. For any clarification/information, Advisor (QoS) may be contacted at Tel. No.+91-11-23230404, Fax: +91-11-23213036.

Contents

Chapter 1

Background to the consultation process

1.1 Background

1.1.1 In the last few decades, the Internet has emerged as an important resource for innovation and economic growth and as a medium to support information exchange within and across borders. The Internet has attained a size unrivalled by any other network by several orders of magnitude. It has come to be created by the cooperative efforts of several stakeholders, but is controlled in its entirety by none. The future growth of telecom sector and of other access networks is contingent upon innovation in web content and the Internet itself. However, increasingly, concerns have been raised globally relating to discriminatory treatment of Internet traffic by access providers. These concerns relating to nondiscriminatory access have become the centre of a global policy debate, often referred to as the Net Neutrality (NN) debate.

1.1.2 In the Indian context as well, there have been multiple consultations on the issue of NN and its related aspects. The following timeline describes initiatives taken by the Authority as well as the Department of Telecommunications(DoT) on the subject:

Table 1.1: NN: Timeline of related activities

19th of Jan 2015	Creation of DoT committee on NN.
27th of Mar 2015	Consultation on regulatory framework for over-the-top (OTT) services.
May 2015	Release of DoT committee report on NN.
9th of Dec 2015	Consultation on differential pricing for data services.
8th of Feb 2016	Regulation on prohibition of discriminatory tariffs for data services.
3rd of Mar 2016	DoT sought Authority's recommendations on NN.
19th of May 2016	Consultation on free data.
30th of May 2016	Pre-consultation on NN.
19th of Dec 2016	Recommendations on provisioning of free data.

1.1.3 As highlighted above, the DoT had sought TRAI's recommendations on issues relating to NN during previous year. The ongoing consultation process was initiated pursuant to this reference from the DoT. The present consultation paper is accordingly being issued in continuation to the "Pre-Consultation Paper on Net Neutrality". In view of the complexity of the subject of NN, the Authority decided to undertake a two-stage consultation process. The first stage, of pre-consultation, was an attempt to identify the relevant issues in all the areas on which the DoT had sought TRAI's recommendations. In this next stage, the Authority has considered all the relevant issues identified during the pre-consultation process and the preliminary inputs gathered from stakeholders on those issues. The purpose of this second stage of consultation is to proceed towards the formulation of final views on policy or regulatory interventions, where required, on the subject of NN.

1.2 Issues raised in the pre-consultation paper

1.2.1 TRAI had, in its pre-consultation paper dated 30th of May 2016 discussed issues such as the definition of NN, scope of traffic management practices, importance of unrestricted access and transparency, need for preserving customer privacy and national security. The pre-consultation paper also highlighted salient points of the recommendations made by DoT's High Level Committee constituted on the same subject in May 2015. In addition to this, the paper listed various regulatory approaches seen world wide in the treatment of NN issues, with a detailed account of the approach followed in jurisdictions like the United States, the European Union, Australia, Japan and Brazil.

1.2.2 In the paper, TRAI had recognised that while there are several definitions of NN, the term is generally understood to mean the principle that Telecom Service Providers(TSPs)[1] must treat all Internet traffic on an equal basis, without regard to the type, origin, or destination of the content or the means of its transmission. In recognition of the complex set of issues surrounding this concept and the diverse viewpoints on the subject, the Authority initiated a deeper enquiry into the various issues relevant to the subject.

1.2.3 The following is a summary of the key issues on which inputs or comments were invited from various stakeholders:

i. Core principles of NN in the Indian context and key issues required to be considered so that the NN principles are ensured.

ii. The scope of reasonable traffic management practices and current practices in India which might raise NN concerns.

iii. Policy/ regulatory approach to deal with issues relating to NN.

iv. Precautions required to preserve national security

[1]This term is being used throughout this Consultation Paper to include all licensed providers of Internet services.

v. Precautions required to maintain customer privacy

vi. Comprehensive policy framework for defining the relationship between TSPs and OTT content providers.

1.2.4 The Authority received number of responses to the paper from a broad range of stakeholders, including TSPs, their associations, content providers, civil society organisations, academics and other individuals. These inputs have been taken into account while framing the issues in this consultation paper. In addition, the Authority has also considered the responses to the relevant questions relating to NN that were raised in the consultation paper dated 27th of March 2015. The comments received from various stakeholders during the pre-consultation stage are available on TRAI's website at `www.trai.gov.in`.

Chapter 2

Framework for further analysis

2.1 Scope of present analysis

2.1.1 At the outset it is relevant to clarify that although the DoT had sought TRAI's recommendations on all relevant standpoints covered in the consultation paper dated 27th of March 2015, including issues like economic, security and privacy aspects of OTT services, the Authority has chosen to focus the scope of this consultation paper on the core areas of NN. As the issues relating to policy framework, including regulation, economic, security and privacy aspects of OTT services, were covered comprehensively in consultation paper of 27th of March, 2015, these issues are discussed here only to the extent that they relate directly to one or more aspects of the NN debate. This allows for a more focused discussion on the subject and prevents digressions into other areas, which although important, are not central to the determination of the NN issues at hand. This approach is also in line with the spirit of the reference received from the DoT, where it had sought recommendations that would be relevant *"in arriving at final viewpoint on various aspects and nuances of net neutrality"*.

2.1.2 Next, it is important to clarify the context in which the term "NN" is being used in this paper. As noted above, at present there is no single standard accepted definition of the term and identifying the core principles of NN was, in fact, one of the issues raised in the pre-consultation paper. The term NN was first coined by academic Tim Wu who

stated that it was *best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites and platforms equally.*[1] Most jurisdictions, including those that are said to have adopted a NN framework, however, do not explicitly define this term in their policy/regulatory framework. This idea of equal or nondiscriminatory treatment of content while providing access to the Internet, however, resonates in the principles adopted by them. This is also the context in which this term is being used in this consultation paper.

2.2 Setting out the Indian context

2.2.1 The Authority recognises that the topic of NN has garnered a lot of attention in global policy debates over the last few years. A number of jurisdictions, developed and developing, have seen extensive discussions on various aspects of this subject while considering their approach towards potential discrimination in access to content on the Internet. As a result, we are now in a position where a wealth of information on NN is already available, both in terms of academic literature and stakeholder perspectives. In addition, the Authority has also gathered a lot of pertinent information from stakeholders in India in the course of its consultations. This may prompt some to question whether any additional value will be gained by undertaking further consultations on this subject in India. It is therefore pertinent to highlight the following points that have been considered by the Authority while adopting its current approach:

i. First and foremost, the two-stage consultation process is designed to give sufficient opportunity to all stakeholders in India, who may not have been part of consultation process held in other parts of the world, to voice their requirements and concerns before the Authority takes a final position.

ii. Second, there are variations in the requirements of one country to another, including in terms of their level of development, adoption of the Internet, state of content business and the regulatory, licensing and legal framework within which they operate. The level of

[1] Tim Wu, Network Neutrality FAQ, available at `http://www.timwu.org/network_neutrality.html`.

market competition among TSPs providing Internet access services is also a key aspect. All of these factors could have influenced the manner in which a country may have dealt with similar issues. In summary, there is no universal approach or global consensus on the best approach to be followed.

2.2.2 Accordingly, authorities in India must, while being informed by the options that have already been exercised elsewhere, develop an approach that is best suited to the Indian context. The attempt in this consultation process is to rethink the first principles of traffic management by TSPs and the contours of reasonableness so as to arrive at an understanding of the principles that we may want to adopt. The following are some relevant factors to be kept in mind in this regard.

i. *Regulatory structure*: In India, issues of licensing and allocation of spectrum are dealt with by DoT while regulatory aspects are dealt with by TRAI. Moreover, the Telecom Regulatory Authority of India Act, 1997 (TRAI Act) confers direct responsibilities on the Authority on some aspects such as determination of tariffs and quality of services, while on others it has only recommendatory powers.

ii. *Licensing regime*: India is divided geographically into many licence service areas and the boundaries of these areas may vary for different types of license. As a result, within the boundaries of India an end user may use data services while roaming on a network which is different from their home network. In the context of a NN framework, this requires determination of the appropriate duty-bearer and the allocation of responsibilities between networks.

iii. *Share of wireless network*: Starting from a few million connections in 1997, India now has more than a billion connections, with almost 98 percent of them being wireless subscribers. The same is also true in terms of the profile of Internet users in the country.

iv. *Demand versus traffic carrying capacity*: In case of wireless networks, traffic demand can be quite unpredictable because of various factors, including the mobility of the user. Capacity of the network may be enhanced by network densification, higher spectrum

bandwidth and the use of spectrally efficient technologies. However, some relevant factors for India include, spectrum constraints, as compared to other countries; and the fact that densification of the network may be constrained by infrastructure (e.g electricity), right of way (ROW) issues, common utility duct and other factors.

v. *Broadband coverage*: The penetration of broadband services (defined to be speeds above 512 Kbps) is still at a preliminary stage compared to many other countries. At the end of September, 2016, the number of broadband subscribers stood at 192.30 million. Of them, 173.87 million were users of mobile devices (phones and dongles). Further, we also see a fair degree of concentration in the hands of the larger players – in September, 2016, the top five service providers constituted 78.62 percent of market share of the total broadband subscribers.

2.3 Towards an appropriate approach for India

2.3.1 Having identified the India-specific context, the next challenge is to examine what should be India's policy response on issues relating to any form of discriminatory treatment in the provision of access to the Internet. The Authority has identified the following as some key issues that need to be deliberated further and finalised before taking a position in this regard:

i. *Understanding various traffic management practices*: Service providers generally use a range of techniques to manage the safety, security and efficiency of their networks. It is important to ensure that such techniques are not used by service providers in a discriminatory manner. However, any such NN policy/regulatory framework should not interfere with the ability of service providers to manage their networks in a reasonable and fair manner. There can be two policy/regulatory approaches to achieve this end. First, a broad approach which involves defining what would constitute "reasonable" traffic management practices. The reasonable traffic management principles would therefore set out the contours of what can be regarded as acceptable or unacceptable forms of interference by a service provider with Internet traffic that flows on its network. In

contrast, a narrow approach would limit itself to a negative list of non-reasonable traffic management practices. Further, this reference to reasonable management of "Internet traffic" also brings into the question the treatment of specialised/ managed services that are delivered using IP but do not serve the same functionality as the public Internet; or those that may require a level of quality that cannot be guaranteed on the Internet.

ii. *Defining the core principles of NN*: Authorities in India are yet to take a final view on whether and how the term NN should be defined for the purposes of our legal/ regulatory framework. Based on review of various reasonable and non-reasonable traffic management practices in the Indian context, it is important to identify core principles of net neutrality for India and the types of practices that might be regarded as being in violation of these core principles.

iii. *Transparency requirements*: While laying down the permissible scope of reasonable traffic management practices, it is important to ensure that the end users who are affected by these practices have access to relevant information about the types of traffic shaping practices being followed by service providers and the reason for which they are being deployed. This information may be required by them in their capacity as consumers or potential consumers of a TSP; as producers of content who might want to reach out to a TSP's consumers; as other TSPs competing in the same line of business; or as members of the general public. It is therefore important to identify the specific transparency-related obligations that need to be followed in each of these circumstances and the point at which such requirements will be triggered.

iv. *Monitoring framework*: Establishing an appropriate framework to monitor and enforce the principles of NN is vital to achieving its objectives. Given the rapid changes in technology, evolving regulatory/ policy environment and fast-developing business models, we need a monitoring mechanism that can remain relevant and appropriate through these changing circumstances. Therefore, depending on the instrument that we use for adopting NN principles in India, the monitoring responsibilities can vary from a situation where the primary responsibility remains with the Authority and other government agencies, to one where we consider other participative /collaborative models for moni-

toring and sharing of compliance information. A combination of these models can also be used.

v. *Policy/regulatory instruments*: Following a discussion on the above issues, the Authority will also need to consider the range of instruments that can be used for giving effect to any NN framework in India. For instance, this can be achieved through voluntary commitments to be agreed upon by TSPs, under the guidance of the Authority; or through the adoption of more specific policy/ regulatory instruments. The latter category could include instruments like a recommendation on introducing a legislation on the subject; amending the terms of the licence agreement to cast NN obligations on TSPs; and formulation of net neutrality regulations by the Authority, using the powers to regulate on the subject of Quality of Service (QoS) that have been conferred on it under the TRAI Act.

2.3.2 In this Consultation Paper, the Authority has fleshed out the above issues in more detail and proposed its formulation for a regulatory approach that can be adopted in each case. The goal is to gather relevant feedback from all categories of stakeholders on the issues identified by the Authority and its proposals on them. In summary, we need to proceed from stage of deliberation on these issues to coming up with specific regulatory/ policy suggestions, if required, and establishing appropriate institutional frameworks to govern them.

Chapter 3

Traffic Management

- Service providers generally use a range of techniques to manage the safety, security and efficiency of their networks. On one hand, it is important to ensure that such techniques should not be used in a discriminatory manner. On the other, any restrictions imposed on TSPs should not interfere with their ability to manage their networks in a reasonable and fair manner.
- There could be two policy/regulatory approaches to achieve this end. First, a *broader approach* may involve defining what would constitute "reasonable" traffic management practices (TMP). As such, the principles on reasonable TMP would set out the contours of what can be regarded as acceptable and unacceptable forms of interference by a service provider with the Internet traffic that flows on its network. In contrast, a *narrow approach* would limit itself to a negative list of non-reasonable traffic management practices.
- Certain exceptions might need to be carved out, such as for prioritising emergency services or complying with directions regarding unlawful content.
- The reference to reasonable management of "Internet traffic" also brings into question the treatment of specialised/ managed services that might not serve the same functionality as the public Internet; or may require a level of quality that cannot be guaranteed on the Internet in the normal course.

3.1 Need for traffic management

3.1.1 As discussed in the pre-consultation paper, the proliferation of a vast variety of applications, websites, and other forms of content on the Internet, has enhanced user choice and paved the way for greater innovation and competition. However, a fundamental feature of the Internet is that it operates on a *best efforts* basis. This means that the TSPs do not guarantee either the time of delivery of each and every data packet transmitted over the Internet or even the fact of such delivery.

3.1.2 At the same time, we know that the diverse range of content available on the Internet has varying characteristics, uses and bandwidth requirements. For instance, some content (like video) requires high bandwidth whereas some applications (like real-time gaming) have very stringent requirements. The exponential increase in Internet traffic and the evolving nature of the content that constitutes part of this traffic, can therefore lead to the overburdening of networks. As a result, TSPs may not always be able to deliver an adequate level of QoS to their users, which is problematic both from a regulatory compliance perspective as well as for competitive reasons. Firstly, the regulations put in place by the Authority require the TSP to adhere to certain QoS benchmarks that are regarded as basic indicators of the satisfactory performance of the network. For instance, TRAI's Standards of Quality of Service for Wireless Data Services Regulations, 2012 put in place requirements relating to average "latency", which refers to the time taken by a packet to reach the receiving endpoint once it has been transmitted. Secondly, competitive forces also drive TSPs to manage their networks in a manner that is conducive to attracting new customers and retaining existing ones by offering them a satisfactory user experience. As a result, TSPs tend to deploy various types of traffic management techniques on their networks in order to meet the demands for delivering a satisfactory QoS. This is often done by taking into account the specific nature and needs of the data packets being transmitted. TMPs are, therefore, used to optimise overall network performance and maintain a consistent QoS for users while carrying a diverse variety of traffic over the networks.

3.1.3 The use of traffic management tools acquires a particular relevance in the Indian context, since a majority of Internet usage is through wireless networks. As of September 2016, India had a total telecom subscriber base of 1074 million out of which 1049 million subscribers were on wireless networks. Limited spectrum availability is an enormous constraint in case of wireless network capacity. As highlighted by some responses to the pre-consultation paper, managing wireless networks poses a bigger challenge on account of spectrum constraints, sensitivity to interference, physical obstructions, lower indoor coverage and varying number of active users. Specialised traffic management and optimisation techniques are therefore required in such networks, which may be different from those used for fixed wireline services. Any review of such TMPs should therefore take into account differences in network architecture and technology.

3.1.4 Some of the common reasons for which TMPs may be deployed are discussed below:

- **Traffic congestion:** In case of network overloads, it may sometimes become important to prioritise/throttle one content stream over the other until the congestion is resolved. While enhancing network capacity would reduce instances of traffic congestion, there may still be situations of network overloads that are unpredictable, irregular and temporary, where TMPs could need to be employed to ensure consistent connectivity and QoS for users. As discussed above, this is particularly relevant in case of wireless networks.

  Peak-load management: A particular case of traffic congestion would be instances of peak-load on the network. Due to various factors like activity of users, bandwidth heavy applications and content and mobility of users, a network may experience a peak of Internet usage in particular area within a specific time window. The peaks in Internet activity can be characterised into daily peaks, weekly peaks, monthly peaks and seasonal peaks. TSPs may find it challenging to strike the right balance in such cases because networks designed to meet the requirements of all-time peak shall remain significantly underutilised as the peaks occur only for a short duration and that too occasionally. On the other hand, if wireless network capacity is not designed to meet

all-time traffic peak then degradation of QoS and user experience may be observed in situations where demand exceeds capacity.

- **Prioritisation of latency-sensitive traffic:** Some Internet traffic like VoIP is latency sensitive and requires continuous connectivity. In addition, such traffic may also require certain minimum QoS. In case of limited network capacity, a TSP might feel compelled to prioritise the latency sensitive traffic over the less sensitive one.

- **Network security and integrity:** TSPs may need to deploy TMPs in order to protect their networks from viruses, spam, denial of service attacks, hacking attacks against network/terminal equipment, malicious software etc. These activities have the potential to harm both the network and end-users.

- **Legal requirements:** TMPs may be required to be used to comply with court orders and restrictions imposed by the government or law enforcement agencies.

- **Emergency:** During a time of emergency situations, TSPs may have to resort to TMPs in order to manage Internet traffic and prioritise urgent communications or content.

3.1.5 Apart from the reasons mentioned above, some stakeholders have highlighted the use of TMPs for user-defined reasons – like blocking of a certain content to implement parental control over access to undesirable material. In addition, recent research indicates the possibility of new technologies that allow end users to tell TSPs and content providers when and if they want certain content to be given preferential treatment.[1]

3.1.6 It is pertinent to reiterate that some problems like traffic congestion and peak-load management should ideally be addressed by enhancing the overall network capacity. But, even in a situation of enhanced capacity, some degree of scarcity might persist and therefore, TMPs might still play a role in efficiently delivering services to end-users. Stakeholders

[1]Tom Abate and Glen Martin, Stanford engineers propose a technology to break the net neutrality deadlock, Stanford News Service, September 13th 2016, available at http://news.stanford.edu/press-releases/2016/09/13/breaking-net-neutrality-deadlock/

present a a range of differing views in this regard. In the pre-consultation responses, one organisation has noted that reasonable traffic management must be strictly limited to circumstances of unpredictable load and should not be used as a cover for systemic underinvestment in network capacity. Another respondent has, however, stated that even though investments in network capacity are essential to support the exponential growth in IP traffic, more capacity will not reduce the need for traffic management. It will also not address the latency, throughput and jitter needs of different services/content.

3.2 Why "reasonable"?

3.2.1 All stakeholders, however, seem to be in agreement that TSPs must have the flexibility to manage their networks in an efficient and reasonable manner. As discussed above, there are several reasons for TMPs such as congestion management, ensuring the integrity and security of the network, and implementing court orders or emergency communications. TSPs have the incentives to ensure that their networks are managed in a manner that offers the best possible experience to a large number of users using different categories of content. However, the same commercial considerations that prompt TSPs to use TMPs to improve network performance can also become the cause of certain exclusionary or discriminatory practices. For instance, vertical integration or partnerships with content providers are increasingly being seen as one such source of additional financing or strategic engagement for TSPs.

3.2.2 Globally, there are several examples of TSPs interfering with their networks by using TMPs to carry out service blocking, prioritising affiliated content provider services or throttling competing ones. Several stakeholders have also pointed to the emergence of similar practices in the Indian context. It is argued that his trend of differentiation of traffic by TSPs based on content is a function of their ability and incentive to interfere with the network in ways that might impede user choice. These practices can also distort competition in the content provider business, thereby discouraging present and future innovation. If permitted, they could tilt the playing field in favour of companies with the ability to form partnerships with TSPs, often on account of their deep pockets, and TSP-owned content

companies. Similarly, there is also a concern that TMPs may be used as a tool to preserve legacy systems at the cost of new technologies that may be able to deliver more useful or affordable solutions for users.

3.2.3 It is in this context, that a discussion on NN emerges. It can be summarised to mean the debate surrounding the need for a policy/regulatory framework for ensuring nondiscriminatory treatment of content by TSPs. The aim is to restrict TSPs' ability to interfere with the network in ways that hamper innovation and restrict user choice, while allowing them to retain the flexibility to manage their networks in an efficient manner.

3.2.4 The resolution of these issues is closely related to TRAI's policy objectives of protecting the interests of consumers and ensuring orderly growth of the sector. The growth of the Internet has had a cascading effect on multiple other sectors of the economy, both commercial businesses and different components of the social sector. Innovation on the Internet and ensuring its openness is, therefore, critical not just for the direct users of Internet access services but also all the providers and users of numerous services that are built around the Internet ecosystem. This makes it all the more important to draw a balanced response to the questions of how we allow data traffic to flow on the Internet and the ability of any one set of stakeholders to shape the nature and flow of that traffic.

3.2.5 At the same time, TRAI is also concerned about taking into account the interests of service providers, once again with the objective of protecting the interests of the sector as a whole. This gives rise to the need to consider the balance between allowing TSPs to manage their network in a reasonable manner versus their obligation to do so in nondiscriminatory manner. In the absence of such a balance, any policy/regulatory framework could create disincentives to network investment and capacity generation.

3.2.6 Thus, a discussion on NN must begin by identifying what constitutes reasonableness in the context of TMPs, and identifying those practices that deviate from such standard.

3.3 Identifying the relevant "traffic"

3.3.1 In order to clarify the ambit and duty-bearers under any reasonableness standard, it is essential to first understand the contours of the "traffic" that is sought to be covered within the scope of the present discussion. For this purpose, it is important to identify the meaning of Internet services and the persons who are regarded as being providers of such services. For instance, should the application of any TMP standards be limited to providers of last-mile Internet access services or should any other categories of persons also be included within its scope.

3.3.2 The Unified Access Service License (UASL) in India defines the "Internet" to mean a global information system that is linked together by a globally unique IP address and is able to support communications using the TCP/IP suite or other IP compatible protocols. The terms of the license identify the scope of services that can be offered by a licensee that is authorised to provide "Access Services" or "Internet Services". These include, *"Internet Telephony, Internet Services including IPTV, Broadband Services and triple play i.e voice, video and data"*. The term "Internet Services" itself has however not been explicitly defined.

3.3.3 Other jurisdictions have found it useful to clarify the scope of Internet access services in the context of their NN frameworks. In European Union (EU), the open Internet access regulations define "Internet access service" as a *"a publicly available electronic communications service that provides access to the Internet, and thereby connectivity to virtually all end points of the Internet, irrespective of the network technology and terminal equipment used"*. The law in Brazil defines it as a 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. The Federal Communications Commission (FCC) refers instead to the the term "broadband Internet access service", which it defines to mean *"a mass-market retail service that provides the capability to transmit and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental" to these services.* Critically, the FCC clarifies that the term also encompasses services that

provide "a functional equivalent" to the above-mentioned service, or that which is being used to evade any protections set forth in their order.

3.3.4 The policy/regulatory framework in India may similarly need to consider the scope of Internet access services for the purposes of determining what constitutes reasonable TMP in respect of such traffic. This would involve assessing whether characteristics like *publicly available* communications service; and providing connectivity to *"virtually all" or "all or substantially all"* end points on the Internet or any other criteria should also be used in India.

3.3.5 As a logical corollary to this discussion, any services that do not qualify as "Internet access services" would fall outside the purview of the present discussion. This makes it important to discuss whether there is a need to define this residual category and what are the types of services or arrangements that may be covered in its scope. In its Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016, the Authority has clarified that the regulation does not apply to tariffs for data services over *closed electronic communications networks*, unless these are being used for the purpose of evading the prohibition in the regulation. The accompanying explanatory memorandum to the Regulation clarified that this was meant to include examples such as intranets, which are not used for accessing the Internet.

3.3.6 Some other jurisdictions have used terms like "specialised services" or "managed service" to identify the services that are excluded from the scope of NN regulations. One criteria for defining such services may be that such services may require a guaranteed level of QoS that can not be offered on the public Internet. This is the approach followed by the EU regulations, which exclude services that are *"optimised for specific content, applications or services"*, where such *"optimisation is necessary in order to meet requirements of a specific level of quality"*. Examples include health-care services like tele-surgery, Voice over Internet Protocol (VoIP) and IPTV services.

3.3.7 The FCC on the other hand has observed that the use of the term "specialised services" can be confusing as the critical point is not whether the services are "specialised" but that they are not broadband Internet access services. They give the following as examples of such services – Connectivity bundled with e-readers, heart monitors, energy consumption sensors, limited-purpose devices such as automobile telematics, and services that provide schools with curriculum-approved applications. While choosing not to define the scope of these non-broadband services on the ground that this may limit future innovation and investment, the FCC did however refer to the following general characteristics that were identified by the Open Internet Advisory Committee in the United States:

1. These services are not used to reach large parts of the Internet;
2. They are specific application-level services, and not generic platforms; and
3. They use some form of network management to isolate the capacity being used from that used by broadband Internet access services.

3.3.8 It would be useful to consider if we need to adopt any similar guidelines in the Indian context. In addition, it would also be pertinent to examine how we should treat certain specific types of services, such as the ones highlighted below, while arriving at a formulation of what is included or excluded from the scope of Internet traffic.

1. Enterprise solutions
2. Internet of Things (IoT)
3. Content Delivery Networks (CDN) and interconnection arrangements
4. Virtual Private Network (VPN)

3.3.9 As per the FCC, broadband Internet access service does not include VPN services, CDN, hosting or data storage services, or Internet backbone services, as they do not provide the capability to exchange data with all Internet endpoints. Similarly, the Body of European Regulators for Electronic Communications (BEREC) Guidelines, 2016 suggest that a specific

VPN that offers a "private network", with access to limited endpoints and is secured for internal communications, could qualify as a specialised service. However, if a corporate VPN service also provides access to the Internet, such access would be governed by the EU regulations.

3.3.10 The increasing role of CDN in the delivery of data is an important area that merits discussion while evaluating how traffic should flow on the Internet. Studies have estimated that by 2020, 64 percent of total Internet traffic will be carried on CDN, up from 45 per cent in 2015.[2] Large content providers may also directly host their content inside the TSPs network through direct interconnection arrangements. As noted above, the NN frameworks adopted by some other jurisdictions have clarified that they do not regard such services and arrangements as falling within the scope of Internet traffic. This issue has however not yet yet been fully debated in the Indian NN consultation processes and therefore merits further deliberations.

3.3.11 Lastly, it is also important to consider the safeguards that need to be adopted to ensure that the exclusions offered for any specialised/ non-Internet services are not misused. In some cases this has been done through the adoption of principles to ensure that such services should not be used to circumvent the regulations; and should not negatively impact the availability or performance of general Internet access services. Providers are required to present specific disclosures in this regard, as discussed further in the chapter on Transparency.

3.4 Different policy/regulatory approaches for TMP

Having referred to the importance of ensuring reasonableness in the application of TMPs and of identifying the relevant traffic to which any such standards would apply, the next step is to consider the policy/regulatory approaches on what these standards could be.

[2]White paper: Cisco VNI Forecast and Methodology, 2015-2020, 6 June, 2016, available at `http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html`.

3.4.1 Broader approach: Defining reasonableness In several jurisdictions with NN frameworks, the reasonableness of traffic management is tested on two concurrent grounds. First, that the measure should be technically motivated to address network congestion, or the integrity or security of the network; and must follow certain guiding principles like proportionality and nondiscrimination. Second, that it should not be based on commercial considerations or practices.

Technical reasons for TMP

i. In the EU regulatory framework, TMP must be *"based on objectively different technical QoS requirements of specific categories of traffic"*, while the US Open Internet Order states that permissible TMP is one that has a *"primarily technical network management justification"*.

ii. *Categories of traffic:* In order to identify when TMP is based on legitimate technical reasons, an understanding of different categories of traffic and their technical QoS needs may be required. In their submissions to the pre-consultation paper, stakeholders presented differing views on how to identify classes of traffic for this purpose. Some stakeholders stated that the definition of classes should be set out by the regulator and not be left to the TSPs, while others proposed that operators themselves should be allowed the flexibility to create these classes and rate them on a scale to prioritise delivery of services.

iii. *Application-specific discrimination:* The other distinction worth noting is that in the treatment of discrimination in respect of a particular application within a class/category of traffic (say, a particular application among high-quality video calling services); as compared to discrimination amongst classes/categories of traffic (say, serving video content at a slower speed than non-video content). Some stakeholders take the view that the former case should be viewed more strictly as it is clearly discriminatory and a strong indicator of commercial motivations. On the latter case, while some others believe that video content, which is bandwidth intensive, may pose greater congestion challenges than other content and therefore would require differential treatment, others pointed out that this should be addressed in a proportional and temporary manner, rather than

permanently discriminating against video content. This points back to the principle that TSPs must deliver all traffic on a "best-efforts" basis irrespective of the category of traffic.

iv. *Proportionality:* Regulations adopted by the EUrequire that any TMPs must be deployed in a manner that is "transparent, nondiscriminatory and proportionate". Their proportionality standard frames reasonable TMP as practices that occur in order to respond to exceptional circumstances (*"except as necessary"*); and should therefore be temporary and the least restrictive means possible ("*only for as long as necessary*"). Further, the BEREC Guidelines, 2016 recommend that even legitimate TMP should be carried out using the least restrictive means – both by limiting TMP to the *"section of the network where congestion occurs, if feasible"*; and by considering whether throttling, as opposed to blocking of traffic would be *"sufficient and equally effective to manage congestion"*.

v. *Encrypted content:* Some stakeholders have submitted that discrimination based on the "features" of content should also be discouraged. For example, encrypted traffic should not be discriminated against as it is not a barrier to traffic management, and would create perverse incentives to avoid such a privacy and security enhancing technology. In the EU context, the BEREC guidelines clarify that the fact that traffic is encrypted is not a legitimate reason for ISPs to throttle such content. Similarly, prioritising locally cached content claiming it to be reasonable network management while not allowing other content providers to cache traffic locally could pose a concern.

vi. *Deep packet inspection (DPI):* On the issue of identification of the different data packages for the purposes of traffic management, some operators have pointed out that this is required so that packages that are more critical or require a greater transmission capacity can be prioritised during congestion. Other stakeholders like civil society organisations (CSOs), academics and several individual respondents are however in broad agreement that practices like DPI should not be used for gaining unlawful access to the type and contents of an application in an IP packet. One operator also noted that TSPs should be mandated to get permission from relevant authorities before carrying out packet

inspections. Stakeholders have also expressed their views on this subject in response to the question relating to protection of consumer privacy.

vii. *Security of the network:* As noted, allowing TSPs flexibility to respond to threats to the security of the network is important in the interests of the network, and its end-users. Some jurisdictions have treated such TMP as an exception to any NN rule. The BEREC, however, has noted that this exception could be used to circumvent the EU regulations given that security is a broad concept. Therefore, regulators are encouraged to assess whether the measure was intended at preserving the integrity and security of the network. Further, the principles of proportionality and using the least restrictive means will continue to apply.

Commercial reasons for TMPs

viii. If TSPs are allowed to use TMP to block or slow down specific content on the Internet, they might have the incentive to use this to the disadvantage of (i) third party services like VoIP that compete with their traditional revenue streams; and (ii) other content providers that offer services provided by the TSP, its affiliates or any person with whom it enters into a commercial or strategic arrangement. Further, if TSPs are allowed to charge content providers for reaching their users it could lead to them exercising a gatekeeping function. In such a situation, TSPs might find it attractive to restrict access of some content providers as a way to earn more from other content providers that have a higher willingness to pay.[3] It could also create an incentive for the ISP to maintain a level of scarcity, thereby maximising gatekeeping revenues.[4]

ix. For these reasons, all jurisdictions that have adopted NN policy frameworks recognise that TMP should not be motivated by business or commercial agreements. The EU regulation states that TMP *"shall not be based on commercial considerations"*, while

[3]S.Greenstein et al, Net Neutrality: A Fast Lane to Understanding the Trade-Offs, Journal of Economic Perspectives, 2016

[4]Tim Wu et al, Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality, Journal of Economic Perspective, 2009

the FCC's Open Internet Order states that reasonable TMP *"does not include other business practices"*.

x. Although commercially motivated TMP are held to be immediately suspect across jurisdictions, it is not a precondition to the finding of a violation. For instance, the BEREC Guidelines, 2016 state that *"regulators need not prove that traffic management is based on commercial grounds, it is sufficient to establish that the traffic management measure is not based on objectively different technical QoS requirements."*

3.4.2 Narrow approach: Identifying restricted TMPs

i. Some TSPs and others have pointed out that any restrictions on traffic management should be principles-based and not prescriptive so that it does not hinder the future development of networks. As such, the former approach which lays down the contours of what qualifies as permissible TMP might be thought of as over-regulation given that Internet access service is a dynamic technology with changing functionalities.

ii. In this regard, another approach could be to not prescribe standards of reasonableness but instead only declare that certain TMPs are not regarded as being reasonable, due to their ability to impede user choice and deter innovation. For example, it could be stated that any TMP that is commercially motivated would be regarded as being discriminatory, and is therefore barred. Under this approach, it is assumed that TSPs have a legitimate interest in managing their network, and the policy/regulation will only specify prohibited activities stemming from particular kinds of commercial agreements or relationships.

iii. In the narrow approach, it may not be necessary to lay down details of identification of classes of traffic, or what will count as objective or technically motivated measures. It may be argued that this brings about more certainty in the policy framework. However, this approach can also present the following challenges:

- Firstly, any narrow approach will be tailored specifically to address the specific challenges that we are aware of today. This may motivate providers to develop

other types of business practices that are not explicitly covered in the narrow restrictions although they may have similar harmful effects.

- Secondly, in the example referred to above, lack of commercial motivation could be seen as a sufficient guide for reasonableness. On the other hand, it has been argued by various stakeholders that TMP should be narrowly tailored and therefore be temporary, exceptional and nondiscriminatory in their effects or application. Moreover, it is argued that TMP should not be used as a cover for systematic underinvestment in network capacity. A broader approach might be better suited to address these aspects.
- Thirdly, in the absence of an agreement or partnership, a commercial motivation might not always be apparent or explicit. In such a case, making the case that a particular measure is discriminatory would be challenging. On the other hand, the broader approach could use specific principles to assess the discriminatory treatment of traffic (whether it is objective, temporary and proportional) and accordingly arrive at a conclusion on its reasonableness. This might be useful for identifying those TMP that are discriminatory in effect but not evidenced by an explicit commercial agreement or partnership.

3.4.3 Approach of DoT's committee The recommendations of the DoT Committee appear to take the broader approach to understanding reasonable traffic management. They state that legitimate traffic management practices may be allowed subject to the core principles. The general criteria against which these practices can be tested may *inter alia* include:

- Adequate disclosure to users about traffic management policies and tools to allow them to make informed choices.
- Application-agnostic controls may be used but application-specific control within the "Internet traffic" class may not be permitted.
- Practices like deep packet inspection should not be used for unlawful access to the type and contents of an application in an IP packet.

- Improper (paid or otherwise) prioritisation may not be permitted.

Thus, the DoT Committee recommended a framework that goes beyond testing for commercial motivation ("paid or otherwise") to broader principles of transparency and nondiscrimination. They also took a strict view of prohibiting application-specific controls, while suggesting that application-agnostic controls could be utilised.

3.5 Exceptions

3.5.1 Prioritisation of emergency services: Emergency services or services used during emergency situations could be an exception to any restrictions on TMP. This will require defining such services and the mechanism through which such exception will be triggered. For example, the law in Brazil allows discrimination of traffic if it *"is deemed essential for the prioritization of emergency services"*. Authorities in Brazil have recently initiated a consultation process to narrowly tailor the definition of emergency services.

3.5.2 Lawful content: It is commonly accepted that the requirements of NN apply only in respect of access to lawful content. This implies that a TMP to, say, block content pursuant to a direction from authorities authorised by law to do so, and after following due process – will not be considered unreasonable. This, however, does not put any positive obligation on TSPs to verify the lawfulness of the content or discriminate among content based on its lawfulness.

3.5.3 Government notified content: There might be certain services that could be notified as an exception to reasonable TMP standards in public interest by the Government/ Authority, based on certain criteria. Such criteria would have to be narrowly tailored to prevent misuse. There might also be concerns relating to competitive neutrality that would have to be addressed in situations where the notified services operate in a competitive market environment.

3.6 Issues for consultation

Q.1 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.

Q.2 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).

Q.3 If a broad regulatory approach, as suggested in Q2, is to be followed:

(a) What should be regarded as reasonable TMPs?

(b) Whether and how should different categories of traffic be objectively defined from a technical point of view for this purpose?

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

(d) How should preferential treatment of particular content, activated by a users choice and without any arrangement between a TSP and content provider, be treated?

Q.4 If a narrow approach, as suggested in Q2, is to be followed what should be regarded as non reasonable TMPs?

Q.5 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.

Chapter 4

Core principles of Net Neutrality

- Based on a review of various reasonable and non-reasonable traffic management practices in the Indian context, it is important to identify core principles of net neutrality for India and the types of practices that might be regarded as being in violation of these core principles.
- The relationship between these core principles and reasonable traffic management standards will also need to be considered.
- In addition, it would be useful to identify whether any specific practices, such as blocking, throttling or preferential treatment of content, need to be specifically dealt with in the NN related framework.

4.1 Defining network neutrality

4.1.1 In light of the discussions in the previous chapter it is clear that TSPs need to employ a range of available tools in order to manage their networks in a reasonable and efficient manner. Accordingly, countries that have adopted any form of NN principles have taken varying approaches on i) identifying the relevant NN principles in their context; and ii) balancing NN with reasonable TMPs in their regulatory frameworks.

4.1.2 The idea of equal or nondiscriminatory treatment of traffic that flows on the Internet resonates in the NN principles adopted by various jurisdictions, although the term itself does not necessary feature in their regulatory instruments. The EU regulations, for instance, create *"common rules to safeguard equal and nondiscriminatory treatment of traffic"* without expressly using the term NN.[1] Given that key terms such as "equal treatment" are still contested, many have urged against a rigid definition of NN. This was also the view expressed by the DoT Committee in its report, where it stated that *"the crux of the matter is that we need not hard code the definition of Net Neutrality but assimilate the core principles of Net Neutrality and shape the actions around them"*. The Committee suggested the following as guidelines to define these core principles:

1. User rights - Subject to lawful restrictions, the fundamental right to freedom of expression and nondiscriminatory access to the internet will apply.

2. Content - Right to create and to access any legal content, applications or services without any restrictions

3. Devices - Freedom to connect all kinds of devices, which are not harmful, to the network and services

4. Harmful practices - Practices like blocking, throttling and improper (paid or otherwise) prioritisation may not be permitted.

4.1.3 In a similar vein, most countries have rooted their NN frameworks in the rights of users to choose content without interference from TSPs and the principles of nondiscrimination and application agnosticism. The FCC, while recognising maximizing end-user control to be a policy goal, noted that *"letting users choose how they want to use the network enables them to use the Internet in a way that creates more value for them (and for society) than if network providers made this choice for them"*.[2]

[1]The Body of European Regulators for Electronic Communications (BEREC) however does use the term Net Neutrality in its guidelines.

[2]Federal Communications Commission, "Preserving the Open Internet. Report and Order", 2010

4.1.4 Several countries, including the US, EU, Norway and Chile have put in place the core principle that end user's have a right to send or receive information/content irrespective of the content, source or destination of packets being transmitted. For example, the EU regulations provide for the safeguarding of nondiscriminatory Internet access by laying down that:

1. End-users[3] have the right to (i) access and distribute information and content; (ii) use and provide applications and services; and (iii) use terminal equipment of their choice. These rights apply irrespective of the end-user's or provider's location or the location, origin or destination of the content being accessed on the Internet.

2. Providers of Internet access services should treat all Internet traffic *"equally and without discrimination, restriction or interference"*. Being treated equally and without discrimination is defined as treatment that is independent of the (i) sender and receiver; (ii) content applications or services; or (iii) terminal equipment being used.

In addition to these core principles, the EU specifically prohibits agreements between TSPs and end-users on characteristics *"such as price, data volumes or speeds"* and any commercial practices of TSPs that limit the exercise of the end-user's rights.

4.1.5 Thus, flowing from this end-users right is a corresponding obligation on providers of Internet access to treat all data packages on a nondiscriminatory basis. In the EU, the obligation is one to *"treat all traffic equally"* and *"without discrimination"*, whereas in the US it is a general obligation not to cause *unreasonable interference/disadvantage* the ability of user/edge providers to use Internet access services to reach one another, thus causing harm to the open Internet.

4.1.6 While several countries have specifically clarified that the guarantee of nondiscriminatory access applies irrespective of the terminal or equipment used, there are some stakeholders who raise the concern that the quality of Internet experienced by a user is often impacted by

[3]As per BEREC, the term "end-user" encompasses all individuals and businesses, including consumers as well as content and application providers.

the type of device being used. In addition, factors such as the browser or operating system being used can also determine the user's experience. This might prompt the question of whether issues such as "device neutrality" should be considered within an NN context.

4.2 Restricted practices

4.2.1 In addition to the general core principles detailed above, several countries specifically prohibit certain practices that are regarded as being violations of such core principles. The US is one such prominent example of a jurisdiction that lays down bright-line rules prohibiting practices of blocking, throttling and paid prioritisation that are "known to harm the Open Internet".

4.2.2 Blocking The FCC Open Internet Order in the US prevents blocking access to *"legal content, applications, services, or non-harmful devices"*, while the Brazilian law on Internet rights refers to a prohibition on *"blocking, monitoring, filtering and analyzing the content of data packets"*.

4.2.3 Throttling This term has been defined in various ways, which includes the following types of interferences in the access to particular content:

- "Slow down, alter, restrict, interfere with, degrade or discriminate" (EU)
- "Impair or degrade" (US)
- "Interfere with, discriminate, hinder or restrict" (Chile)
- "Unreasonable manipulation or degradation of traffic" (Norway)

4.2.4 Preferential treatment In addition to blocking and throttling, some countries also include a bright line rule restricting any form of content-specific preferential treatment. However, the definitions vary. The FCC in the US uses the term "paid prioritisation", where it is required that the prioritisation was either *"(a) in exchange for consideration (monetary or*

otherwise) from a third party, or (b) to benefit an affiliated entity". The DoT Committee in its Report on NN, however recommended that *"improper (paid or otherwise) prioritization may not be permitted"*, without imposing the kind of requirements envisaged in the US law. In Japan the voluntary guidelines prevent *"favourable or unfavourable treatment of specific users"*, which could include both throttling and preferential treatment of content.

While the above mentioned practices are specifically restricted under most NN frameworks, detection of their deployment remains an issue requiring clarity. We need to consider what tests, thresholds and technical tools will be required to detect such practices. For example, while investigating whether a particular application is being throttled, it might be necessary to take into account factors such as QoS parameters for other similar applications, the particular geographical area and the time at which the application was accessed. The use of various statistical methods and QoS measurement tools might also be required for this purpose.

4.3 Link with reasonable traffic management

4.3.1 As noted above, countries also differ in terms of their approach towards balancing the principles of NN with reasonable TMPs. Some countries address it by way of an "exception" to the core principles of NN. For instance, in the US, the FCC has made it clear that *"reasonable network management"* is an exception to the bright-line rules, in recognition of the need for service providers to manage the technical and engineering aspects of their networks. Similarly, in Chile, while the core principle prevents service providers from *"arbitrarily"* interfering with the rights of users, there is a specific exception allowing them to *"take the measures or actions necessary for traffic management and network management... provided that this is not designed to perform actions that affect or may affect free competition"*. The Slovenian law also has a clear exception for *"urgent technical measures to secure the undisturbed operation of networks and services (e.g. avoidance of network congestion)"* as well as *"urgent measures to preserve the integrity and security of networks and services (e.g. removal of undue excessive load on a transmission medium/channel)"*.

4.3.2 In contrast, other jurisdictions do not frame reasonable traffic management as an exception to, or in conflict with, the core NN principles and instead simply clarify that such principles will not prevent the reasonable management of networks. For example, the EU regulation states that the rules *"shall not prevent"* providers of Internet access services from implementing reasonable traffic management measures; and Norway clarifies that *"it does not mean that the principle precludes"* reasonable network management.

4.3.3 Chapter 6 discusses the range of policy options that are available to the Authority at this point of time. Regardless of which approach the Authority chooses to adopt, it is important to recognise that the networks to which these principles are being applied are going through a process of rapid transformation. Accordingly, it is likely that the prevailing circumstances and the Authority's view on them may also evolve in the times to come. Any principles that may be adopted at this point would therefore be subject to ongoing review and analysis of their impact on the sector as a whole.

4.4 Issues for consultation

Q.6 What could be the principles for ensuring nondiscriminatory access to content on the Internet, in the Indian context?

Q.7 How should the following practices be defined and what are the tests, thresholds and technical tools that can be adopted to detect their deployment

(a) Blocking;

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

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

Q.8 The quality of Internet experienced by a user may also be impacted by factors such as the type of device, browser, operating system being used.

How should these aspects be considered in the NN context? Please explain with reasons.

Chapter 5

Transparency

- While laying down core principles of NN and reasonable traffic management standards, it is important to ensure that end users who are affected by these practices have access to relevant information about the types of TMPs being followed by service providers and the reasons for which they are being deployed.
- This information may be required by them in their capacity as consumers or potential consumers of a TSP; as producers of content who might want to reach out to a TSP's consumers; as other TSPs competing in the same line of business; or as members of the general public.
- It is therefore important to identify the specific transparency-related obligations that need to be followed in each of these circumstances, the manner of disclosure and the point at which such requirements will be triggered.

5.1 Introduction

5.1.1 Transparency is one of the key enabling factors towards ensuring adherence to the nondiscrimination principles set forth in any NN framework. Given the significant regulatory capacity required to effectively monitor TSPs' networks, effective disclosure of information

pertaining to TMPs and performance characteristics of a network, enables users as well as the regulator to detect violations.

5.1.2 Moreover, public dissemination of information relating to TMPs can contribute to reducing information asymmetries in the market, thereby leading to a competitive market and pro-consumer behaviour. In most countries with NN frameworks, although regulators have concluded that transparency *alone* might not ensure competitiveness (due to information asymmetries, unequal bargaining power and high switching costs), they acknowledge that transparency obligations do impose both direct and indirect constraints on the ability of TSPs to engage in discriminatory conduct.

5.2 Scope of transparency obligations

5.2.1 In an NN context, the scope of transparency obligations can range from obligations cast upon TSPs to disclose technical information on QoS parameters, to providing high level information that is widely understandable and may enable consumers to make more informed decisions, and detect violations.

5.2.2 The scope of information disclosed typically covers the following aspects - First, *price information and commercial terms* relating to the Internet access service being provided; second, relating to information on the *performance characteristics* of the service being provided; and the third relating to *traffic management practices* deployed by the TSP as well as any other *specialised services/enterprise solutions* being offered. Both the FCC Transparency Notice, 2016[1] and the BEREC Transparency Guidelines, 2011[2](supplementing the disclosure requirements under the Universal Service Directive, 2009) recommend disclosure of information relating to these broad criteria:

[1]FCC Public Notice - Guidance on Open Internet Transparency Rule Requirements (GN Docket No. 14-28) (2016), ("Transparency Notice, 2016")

[2]See, BEREC Guidelines on Transparency in the scope of Net Neutrality: Best Practices and Recommended Approaches (2011), ("BEREC Transparency Guidelines, 2011")

i. **Price information and commercial terms:** This includes information relating to price, with details of full monthly service charges, any promotional rates, duration of the promotional period, and details of any applicable fair use policies, data caps and limits and the commercial terms associated with breaching such data caps or download limits. This would also include the consequences of exceeding any caps or allowances.

ii. **Performance characteristics:** This includes information relating to advertised speed, actual speed, minimum QoS and other service quality parameters such as latency, packet loss and the suitability of the service for real-time applications. The FCC Order recommends separate disclosures for each broadband service on offer (such as 3G or 4G networks separately) and further, that such metrics be measured in terms of average performance over a reasonable period of time and during times of peak usage and related to particular geographic areas.

iii. **Traffic management practices:** This includes disclosures on TMP adopted, including indicating the reasons for such practices (eg. congestion management, bandwidth throttling, preferential treatment of traffic and blocking of traffic); whether such practices are specific to an application or class/category of traffic; and the triggers and time periods that such TMPs are deployed for. This could also include information on data plans being affected, and specific notifications to the particular users being affected.

iv. **Specialised services:** In light of the growing relevance of specialised services, it has been considered relevant to monitor their impact on Internet access services. In particular it may be relevant to collect information from TSPs on what "specialised services"/"enterprise solutions" are being offered to end users, and whether and how such services may affect the last mile capacity available for, and the performance of, Internet services.

5.3 Manner and mode of information disclosure

5.3.1 The primary focus of most transparency obligations, is to ensure that consumers have sufficient information in relation to the services being purchased at the time of signing a contract with the service provider. For example, the EU Universal Service Directive, 2009 requires service providers to provide specified information in a *clear, comprehensive and accessible form* at the time of signing the contract. Similarly, the FCC Open Internet Order, 2015 requires prominent display of disclosures relating to commercial terms, performance characteristics and network management *on a publicly available website and disclosure of relevant information at the point of sale.*

5.3.2 However, in order for the disclosures to be effective, the manner of information disclosure might need to vary depending on the intended audience. Several regulators have recognised this concern. The FCC notes that technical information specifically catering to content providers and device manufacturers is important so that they can develop, market and maintain Internet offerings. However, there is a concern that in case this is done through a single disclosure for both end users as well such content/device providers, it may overwhelm the end-users. In this context, the BEREC Transparency Guidelines, 2011 note that in order to make information understandable to end users *"it might be that less information is better than more information."* In view of this, they propose two approaches that are worth mentioning for clarity:

1. Direct approach where the focus is on TSPs making information available to end users; and

2. Indirect approach where the focus is on TSPs making information available to third parties, who would then provide understandable information to end users.

The BEREC Guidelines recommend that while a direct approach be made compulsory, a combination of both would be ideal.

5.3.3 It should be noted that transparency requirements do impose costs on service providers and as such, proportionality with respect to the scope of disclosure obligations is important. The BEREC Transparency Guidelines, 2011 state that the approach taken should not burden service providers with disproportionate costs. In a similar vein, the FCC Open Internet Order creates as "safe harbour" for disclosures that will be considered effective both for consumers and for third parties like content/device providers. They also specify a specific safe harbour format for disclosure at point of sale.

5.3.4 These obligations are typically supplemented by specific notification requirements to the particular end users that are likely to be affected by any TMP adopted by the TSP (EU Universal Service Directive, 2009). The FCC Open Internet Order, 2015 also expanded the notification requirements to include mechanisms for directly notifying end users if their individual use of a network will trigger a TMP, based on their demand prior to a period of congestion, and that is likely to have a significant impact on their experience of the internet. Specific notices to heavy users by service providers is also encouraged in the Japan Packet Shaping Guidelines.[3]

5.4 Options for consideration

5.4.1 In response to the Authority's pre-consultation paper, most stakeholders, including certain TSPs, have emphasised upon the requirement for TSPs to maintain a certain level of transparency with respect to their TMPs, and other aspects of their network performance. However, with regard to the scope of disclosure, the stakeholders have suggested several alternative frameworks. While some have suggested the adoption of broad guidelines on transparency without prescribing granular data points, others have suggested the provision of extensive information that would provide conclusive evidence relating to any TMP.

[3]See, Guideline for Packet Shaping, Japan Internet Providers Association (JAIPA) Telecommunications Carriers Association (TCA) Telecom Services Association (TELESA) and Japan Cable and Telecommunications Association (JCTA), (2008), ("Japan Packet Shaping Guidelines")

Similarly, with regard to the manner of disclosure, the suggestions range from direct dissemination to the public (through a web-page, or through APIs) to provision of information on a confidential basis to the Authority, which can then compile the information and disseminate it onward in the form of publicly available reports providing a high-level overview of the information provided by TSPs.

5.4.2 The Authority notes that several responses have raised concerns over the level of information disclosure that would be considered useful by users in making informed decisions, without being overtly technical and granular. Further, there are concerns surrounding confidentiality of the data pertaining to TSPs.

5.4.3 It may be noted that some of the information categories under which transparency is being sought in the NN context, may already be covered under the Authority's existing transparency regimes. First, extensive information relating to price and commercial terms such tariff plans and value-added services, are mandated to be disclosed at point of sale and on the TSPs websites. Similarly, with respect to performance characteristics, the Authority has issued QoS regulations which state a list of QoS parameters, with minimum benchmarks for operators to meet, that are being monitored. Transparency on several parameters is being mandated, for example, through provisions that require TSPs to publish minimum download speeds for wireless data plans, and ensure that the minimum download speeds are delivered in line with specified requirements.

5.4.4 However, in view of the unique concerns in an NN context, there may be additional information categories such as on TMPs and specialised services, on which transparency would be desirable. Thus, in view of the responses received, and a review of international best practices, the following possible transparency frameworks as identified in BEREC Transparency Guidelines, 2011, could be considered for further deliberations.

i **Direct Approach:** One possible approach could be to mandate disclosures – covering the above mentioned categories of price information/commercial terms; expected performance characteristics and TMPs – in a prescribed format directly to end-users. This may

be mandated to be displayed prominently at points of sale as well as easily accessible on the TSP's website. An indicative format for this purpose has been provided in the Table below. The frequency of such disclosure (for eg. monthly or other appropriate temporal cycle) would also need to be considered.

Table 5.1: Information Disclosure Template

Parameter	**Disclosure Template**
Name of Internet plan	*Specify name of plan*
Pricing Details	*Specify service charges for plan, preferably accompanied by links to comparable plans*
Other Terms and Conditions	
What are the download/ upload limits/ data usage caps/ fair usage policies?	*Specify Yes/No; Specify limits if applicable*
Additional charges applicable beyond specified limits/ usage caps	*Specify charges if applicable*
Performance Details	
Device compatibility (Only for mobile broadband)	*Specify device compatibility; Provide link to list of compatible devices*
Coverage (Only for mobile broadband)	*Provide link to coverage map of mobile broadband services*
Typical Upload Speeds	*Please provide range*
Typical Download Speeds	*Please provide range*
Typical Latency	*Please provide range*
Typical Packet Loss	*Please provide range*
Service Limitations and Traffic Management	
Application Specific Traffic Management	
Are any services, content, applications or products always blocked on this plan?	*Specify Yes/No; List out services, content, applications if applicable*
Are any services, content, applications or products always prioritised on this plan?	*Specify Yes/No; List out services, content, applications if applicable*
Are any specialised services provided on this plan?	*Specify Yes/No*
What is the impact of the above on the plan	*Please elaborate on the impact of Application Specific Traffic Management on user experience*

Parameter	Disclosure Template
Application Agnostic Traffic Management	
Are TMPs deployed during peak hours?	*Specify Yes/ No*
What are typical peak hours?	*Specify typical peak hours if applicable; This may exclude unforeseen peaks*
What type of traffic is managed during peak hours?	
Specify type of traffic (e.g. audio streaming, video downloads, P2P downloads, etc.)	*Specify type of TMP (e.g. Blocking/Throttling/Prioritisation) against each type of traffic*
User Triggered Traffic Management	
Are TMPs deployed to manage compliance with limits/ data caps/ fair usage policy?	*Specify Yes/No if applicable*
What are the circumstances under which TMPs are deployed?	*Specify user based triggers for TMPs, if applicable*
What is the impact (extent and duration) of such TMP?	*Specify the impact (change in performance details) and duration of user specific TMPs, if applicable*

ii **Indirect Approach:** Under this approach, in addition to the above disclosures to end-users and other QoS information currently being submitted to the Authority, it may also be useful to provide additional or more granular or technical information on TMPs to the Authority and other third parties who can aid in monitoring and presenting technical information in an understandable manner to users.

5.5 Issues for consultation

Q.9 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 publish such information?

Q.10 Please provide comments or suggestions on the Information Disclosure Template at Table 5.1? Should this vary for each category of stakeholders identified above? Please provide reasons for any suggested changes.

Chapter 6

Policy or regulatory approach for India

- A range of instruments can be used for giving effect to any NN framework in India. In the event that the Authority chooses to adopt specific policy/ regulatory instruments, these might include amending the terms of the licence agreement to cast NN obligations on TSPs and/or formulation of NN regulations by the Authority, using the powers to regulate on the subject of QoS that have been conferred on it under the TRAI Act.
- Establishing an appropriate framework to monitor and enforce the principles of NN is also vital to achieving its objectives.
- At the same time, given the rapid changes in technology, evolving regulatory/ policy environment and fast-developing business models, we need a monitoring mechanism that can remain relevant and appropriate through these changing circumstances.
- Therefore, depending on the instrument that we use for adopting NN principles in India, the monitoring responsibilities can vary from a situation where the primary responsibility remains with the Authority and other government agencies, to one where we consider other participative /collaborative models for monitoring and sharing of compliance information. A combination of these models can also be used

6.1 Reviewing the available options

6.1.1 As discussed in the pre-consultation paper, world over, a number of different approaches have been adopted for dealing with NN, which can be classified into the following categories:

1. *Cautious observation:* The countries following this approach have taken note of NN issues and currently chosen not to take any specific measures to address them.

2. *Tentative refinement:* These countries are following a light-handed approach, with some refinements to their existing regulatory regime governing communication services, but not going so far as to prohibit certain behaviours.

3. *Active reforms:* These countries have sought to prohibit specific behaviours by TSPs, most often subject to an exception for reasonable TMPs. The approach taken by these countries, ranges from the passing of legislation through parliamentary process (eg. Brazil) to regulations (eg. US, EU) to voluntary guidelines (eg. Norway, Japan).

6.1.2 In the Indian context, the Authority has, through its Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016, already barred service providers from directly, or indirectly imposing discriminatory prices for access to data services based on the type of content being accessed. In its explanatory memorandum to these regulations, the Authority has emphasised the importance of maintaining the open and nondiscriminatory character of the Internet. Therefore, the Authority has clarified its position that Internet access services should be provided in a nondiscriminatory manner and without any undue interference with user choice. This principle is also incorporated in the UASL, which mandates that subscribers should have unrestricted access to all content available on the Internet, unless it is restricted by law. The Authority has further evolved its thinking pursuant to its consultation processes and finds that the following are some of the available options at this point.

1. *Wait and watch:* One option could be to follow a wait and watch approach, as is being done in many other parts of the world. This will allow service providers the freedom

to develop their product offerings in a manner that is best suited for the needs of their users, but with the knowledge that these developments are being monitored by the Authority.

2. *Self-regulation:* The next option could be to allow all licensed providers of Internet services to follow a voluntary mechanism for adhering to core principles of NN as identified through this process, with a self-regulatory monitoring mechanism that would function under the overall guidance of the Authority. As seen in the Norwegian example, the appropriateness of such a model depends on voluntary compliance, for which purpose they organise annual stakeholder meetings to monitor the status of NN.

6.1.3 In both these cases, if it comes to the notice of the Authority that service providers are systematically indulging in discriminatory practices like blocking of particular content or providing slower or faster speeds for access to particular services, appropriate regulatory interventions can be immediately adopted, based on the learnings from this consultation process.

6.1.4 These options could, however, pose the following risks. First, there might be a failure or a significant delay in identifying the discriminatory practices being followed by specific service providers. This is because users generally do not have the means or the ability to detect any interference in their access to particular content, particularly, when it is done in the form of selective variation of speeds. Further, at present the Authority has no formal mechanism for seeking such information from consumers, content providers and other members of the public. Second, even when any discriminatory practices do come to light, the Authority may not be in a position to take action against them due to the absence of an empowering legal framework. Third, this may also create some regulatory uncertainty which could affect the business decisions of stakeholders. In light of these factors, the other approach that needs to be considered is the adoption of an ex ante mechanism that restricts any breach of NN principles and lays down the consequences for it.

6.2 Instruments for reform

6.2.1 This section discusses the instruments that can be used for implementing NN principles in India if we choose to opt for a strategy of active reforms. This may involve a self-regulatory model or the use of legal instruments for mandating bright line rules on NN, implemented through transparency, monitoring and consequences for any violation. Although there will be enforcement challenges, the latter approach can help in sending a strong regulatory message to TSPs, while serving the interests of end-user choice, ensuring a level playing field for content providers and facilitating the overall growth of the Internet sector. This approach can be implemented in several ways:

6.2.2 License: Clause 2.2(i) of the ISP Licence Agreement provides for access to the Internet and all content available without any access restriction. Similarly, Clause 2.1 of Chapter IX of the UASL provides that *"The subscriber shall have unrestricted access to all the content available on Internet except for such content which is restricted by the Licensor/designated authority under Law."*

6.2.3 In this context, one option that can be considered is the issuance of a recommendation by the Authority to the Government to amend the license conditions to expressly mandate adherence to what are may be regarded as the core principles of NN. The Authority could accordingly recommend amending the license agreement to add an explicit reference to the core principles followed by a general mandate to adhere to *"directions issued by the Licensor/TRAI from time to time"*.

6.2.4 Regulations: As noted in the Explanatory Memorandum to the Prohibition on Discriminatory Tariffs for Data Services Regulation, 2016, *"restrictions on accessing all content on the Internet could take several forms one of them being price based differentiation."* The Discriminatory Tariffs Regulation addressed such price based differentiation by prohibiting discriminatory tariffs for data services based on content.

6.2.5 Affording differential QoS based on content could be another form of restriction on user choice. As per Section 11(b)(v) of the TRAI Act, 1997, the Authority is mandated to *"lay down the standards of quality of service to be provided by the service providers and ensure the quality of service and conduct the periodical survey of such service provided by service providers so as to protect the interests of the consumers of telecommunication services"*. As such, another option could be for the Authority to put in place a regulation prohibiting discriminatory QoS.

6.2.6 QoS is understood to be the main indicator of the performance of a telecommunication network. It determines the degree of satisfaction of a user of the services being offered and the degree to which the network conforms to the standards specified by the Authority. Business practices that create the incentive for TSPs to afford varying QoS based on the content being accessed, might interfere with user choice. This form of interference may include practices of blocking or throttling, or making certain content more attractive to access through preferential treatment of any content.

6.2.7 The adoption of a nondiscriminatory QoS requirements through a regulation could, accordingly, be considered as a tool to prevent distortions in user choice and interference with competition among content providers. In addition to bright line rules to prevent blocking, throttling or any form of preferential treatment, it could also include laying down of the minimum QoS standards to be met by TSPs, irrespective of content.

6.2.8 Another approach may be to put in place an umbrella regulation on NN, with subsections addressing tariff (incorporating the existing regulations on discriminatory tariff), QoS and related transparency requirements.

6.2.9 Legislative changes: The Authority could also make a recommendation to the Government regarding the need to introduce a separate NN legislation. However, the pros and cons of such an approach may need to be considered in light of the powers already conferred on the Authority by the TRAI Act to frame appropriate regulations keeping in mind the interests of consumers, service providers and the sector as a whole.

6.2.10 There may, however, be a case for revisiting some of the enforcement powers under the present law. Levying penalties for NN violations is one of the important tools for deterring TSPs from indulging in such practices and would therefore facilitate more effective enforcement. As per the EU regulation, penalties provided for must be "effective, proportionate and dissuasive". The BEREC guidelines, 2016 mention a variety of enforcement measures available to national regulators in the EU such as issuing cease and desist orders in case of infringement, combined with periodical penalties or fines, in accordance with their national laws.

6.2.11 At present, the Authority has structured a mechanism for imposing "financial disincentives", such as for violations of the Discriminatory Tariff Regulation, 2016 as well as for not meeting QoS benchmarks. For example, under the Quality of Service (Code of Practice for Metering and Billing Accuracy) (Amendment) Regulations, 2013, the Authority can levy a financial disincentive of Rs 1 lakh per week on TSPs for delay in submitting audit and action taken reports. It is for consideration whether a similar mechanism is required for any violation of NN principles.

6.3 Monitoring

6.3.1 Identifying violations of NN will require a robust monitoring and information seeking approach. While transparency with respect to TMPs is critical, it has been pointed out that relying on TSP disclosures to self-report violations may not be sufficient for this purpose. This calls for a need for a proactive monitoring approach, that takes into account TSP disclosures, while also focusing on collection of information from users through complaints, user-experience apps, surveys, questionnaires and from third parties through research studies, news articles, consumer advocacy reports, etc. In addition to this, the authority responsible for monitoring and supervision may also need to adopt other innovative tools for the detection of any violations.

6.3.2 This highlights the key issue of identifying the the body that should be responsible for monitoring and supervision of any NN violations; the tests, thresholds and technical tools that may need to be adopted in order to detect such violations; and finally the actions that this body should be permitted to take in the event of any detected violation.

6.3.3 In the EU, national regulators are advised to "closely monitor" and "ensure compliance" with provisions of their NN regulation. Based on this monitoring process, they are given the option to impose requirements concerning technical characteristics, minimum QoS and other appropriate measures on "one or more" providers. In some countries, proactive monitoring is being supported by the use of Internet measurement platforms. For example, some countries are reported to be using performance testing platforms like SamKnows for traffic monitoring purposes.[1] Further, a report by the UK regulator Ofcom published in August 2015, noted that an approach based on a minimum QoS benchmarks would aid app developers in designing platforms and empower users to better understand their use.[2] The Authority also recognises that better measurement of the end-user experience of QoS is a critical to achieving effective enforcement.

6.3.4 There may be various challenges in this process, such as the technical difficulty in proactively identifying violations, by users or any third party or investigating a TMP that is no longer in use. These technical elements of NN enforcement remain a challenge for regulators worldwide, who are actively engaged in building clarity on such issues. It may therefore be useful for authorities and stakeholders in India to monitor such developments and carry out similar research on these areas to inform policy implementation.

6.3.5 While acknowledging the complexity of TMP, and the dynamic nature of new technologies, one option that could be considered is the adoption of a collaborative approach for reviewing the effectiveness of any NN framework. This could be in the form of a multi-stakeholder initiative to review compliance with NN requirements, facilitate exchange of

[1] SamKnows, Our Regulatory Clients, available at `https://www.samknows.com/regulators`

[2] Ofcom, A Study of Traffic Management Detection Methods & Tools, August 2015 available at `https://www.ofcom.org.uk/research-and-data/technology-research/2015-reports/traffic-management`

information about reasonable TMPs, and address new challenges in implementation.

6.3.6 For instance, the Broadband Internet Technical Advisory Group in the US is a multi-stakeholder organisation that operates as a technical working group for developing consensus on broadband network management practices and other technical issues.[3] In Brazil, the Internet rights law provides that any discrimination or degradation of traffic shall be regulated in accordance with law, "*upon consultation with the Internet Steering Committee and the National Telecommunications Agency*". The Brazilian Internet Steering Committee is a multi-stakeholder body comprising of members from the government, the corporate sector, non-government bodies and the academic community. It has been established through an Inter-ministerial Ordinance for the purpose of coordinating on all Internet service initiatives in Brazil, promoting technical quality, innovation and greater dissemination of services available. In EU, BEREC has published several technical reports based on consultations with a variety of stakeholders.

6.3.7 In keeping with such international precedents, a similar review and coordination process can be considered for India to provide inputs on the technical and operational aspects of implementation of any NN framework. This prompts the need to consider whether such a collaborative initiative would be suitable for India and what should be its design and structure. Some of the questions that need to be addressed in this context include – should it be a multi-stakeholder initiative that consist of representation from TSPs, content providers, consumer groups, civil society; academic/research organisations and any other persons; how should such representatives be selected; and finally, what would be an appropriate role for the Authority or any other government agency in such a structure.

6.3.8 Finally, it is important to recognise that the networks on which we might impose any NN regulations are creatures of evolving technologies. In the backdrop of new technologies

[3]The group has published a report on Differentiated Treatment of Internet Traffic, available at `https://www.bitag.org/documents/Press-Release-Announcing-Publication-of-Report-on-Differentiated-Treatment-of-Internet-Traffic.pdf`

like information centric networking, software-defined networking and mobile edge computing, there are growing discussions on the rise of the "context-aware" network. These may be understood as those networks that dynamically adapt to the needs of devices and applications. The term is used in contrast to the "context-blind" network which has applications adapt to its access characteristics. Accordingly, the Authority's understanding of many of the issues as well as that of stakeholders participating in the consultation process may evolve over a period of time on account of development of more context-aware networks; growth of specialised/non-Internet services and any other changes in the nature of traffic flows on the Internet. It would therefore be useful to also reflect upon the manner in which any mechanisms that may be deployed at present may be updated on account of evolution of technology and use cases.

6.4 Issues for consultation

Q.11 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 detected violation?**
- **(c) If the Authority opts for QoS regulation on this subject, what should be the scope of such regulations?**

Q.12 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).**

Q.13 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?**

Q.14 What mechanisms could be deployed so that the NN policy/regulatory framework may be updated on account of evolution of technology and use cases?

Chapter 7

Issues for consultation

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

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.

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.

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?

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

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

(a) Emergency situations and services;

(b) Restrictions on unlawful content;

(c) Maintaining security and integrity of the network;

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

(e) Any other services.

Please elaborate.

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

(a) Blocking;

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

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

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

(a) Disclosures provided directly by a TSP to its consumers;

(b) Disclosures to the regulator;

(c) Disclosures to the general public; or

(d) A combination of the above.

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

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

Q.10 What would be the most effective legal/policy instrument for implementing a NN 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?

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).

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?

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

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

List of Abbreviations

BEREC Body of European Regulators for Electronic Communications.

CDN Content Delivery Networks.

DoT Department of Telecommunications.

EU European Union.

FCC Federal Communications Commission.

IoT Internet of Things.

IP Internet Protocol.

IPTV Internet Protocol Television.

ITU International Telecommunication Union.

NN Net Neutrality.

OTT over-the-top.

QoS Quality of Service.

TMP traffic management practices.

TRAI Telecom Regulatory Authority of India.

TSP Telecom Service Provider.

UASL Unified Access Service License.

VoIP Voice over Internet Protocol.

VPN Virtual Private Network.