RESPONSE TO TRAI CONSULTATION PAPER

ON

NET NEUTRALITY

BY:

Abhishek Rao

Aniruddh Nigam

Ayush Singh

Pushkal Dubey

Sonali Sharma

Sushmita Som

Swapnasarit Satpathy

Panel Constituted by Law and Technology Society,

National Law School of India University

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY,
BANGALORE

TABLE OF CONTENTS

QUESTION 1. WHAT COULD BE THE PRINCIPLES FOR ENSURING NON-DISCRIMINATORY ACCESS TO CONTENT ON THE INTERNET, IN THE INDIAN CONTEXT? 3

QUESTION 3. IN THE INDIAN CONTEXT, WHICH OF THE FOLLOWING REGULATORY APPROACHES WOULD BE PREFERABLE: 4

A. DEFINING WHAT CONSTITUTES REASONABLE TMPS (THE BROAD APPROACH), OR 4

B. IDENTIFYING A NEGATIVE LIST OF NON-REASONABLE TMPS (THE NARROW APPROACH). 4

QUESTION 4. IF A BROAD REGULATORY APPROACH, AS SUGGESTED IN Q3, IS TO BE FOLLOWED: 5

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? 5

QUESTION 5. IF A NARROW APPROACH, AS SUGGESTED IN Q3, IS TO BE FOLLOWED WHAT SHOULD BE REGARDED AS NON REASONABLE TMPS? 8

QUESTION 6. SHOULD THE FOLLOWING BE TREATED AS EXCEPTIONS TO ANY REGULATION ON TMPS? 8

QUESTION 7. HOW SHOULD THE FOLLOWING PRACTICES BE DEFINED AND WHAT ARE THE TESTS, THRESH- OLDS AND TECHNICAL TOOLS THAT CAN BE ADOPTED TO DETECT THEIR DEPLOYMENT? 11

QUESTION 8. –WHICH OF THE FOLLOWING MODELS OF TRANSPARENCY WOULD BE PREFERRED IN THE INDIAN CONTEXT: [SEE CHAPTER 5] 12

(A) DISCLOSURES PROVIDED DIRECTLY BY A TSP TO ITS CONSUMERS; 12

(B) DISCLOSURES TO THE REGULATOR; 12

(C) DISCLOSURES TO THE GENERAL PUBLIC; OR 12

(D) A COMBINATION OF THE ABOVE. 12

PLEASE PROVIDE REASONS. WHAT SHOULD BE THE MODE, TRIGGER AND FREQUENCY TO PUBLISH SUCH INFORMATION? 12

QUESTION 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] 13

QUESTION 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? 13

QUESTION14. 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. 15

Question 1. What could be the principles for ensuring non-discriminatory access to content on the Internet, in the Indian context?

Internet access services must be application-agnostic and facilitate the freedom of expression. It should not discriminate against *lawful* traffic based on its source, content, or service. The state and private entities have increasing influence on the individual's right to expression. A non-discriminatory approach should treat the internet as a medium for the development of communication tools in the global network, and enable diversity of media without State interference for political reasons by TSPs. Interfering by means of varying internet speeds in accessing certain classes of websites restricts the end-user's choice and unwittingly steers/directs use and enjoyment of the internet, and diminishes content dissemination. Users should also be able to create content or innovate without support or permission from ISPs. Agreements between TSPs and end-users on characteristics such as price, data volume and speed which create differential classes of service must be prohibited.

Further, there should be clear guidelines on the scope of non-discrimination and obligations of net neutrality. If the goal is to open the Internet, there should be a clear demarcation between Internet access services and specialized services which may not benefit from net neutrality.[1] Reasonable traffic management on mobile carriers may differ from those on fixed connections, but non-discriminatory access should apply.

[1] Luca Belli, Primavera De Filippi, 39

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

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

In order to understand the regulatory approach that is suitable to the Indian context, it is important to reframe the potential regulatory approaches in realistic terms of implementation.

The broad regulatory approach, in prescribing principles against which every TMP must be analysed opens the regulatory process to multiple litigations based on defining the exact contours of these broadly stated principles and questioning their applicability to specific facts and specific TMP's.

This becomes problematic at the point in time that the lack of commercial motivation is treated as a principle to be used in the adjudication of the reasonableness of the TMP ["*lack of commercial motivation could be seen as a sufficient guide for reasonableness*", page 25, Consultation Paper]. This leads to an increase in litigation on traffic management practices that exclusively belong to a category sought to be prohibited, for the reasons outlined in Para vii, page 23 of the Consultation Paper.

On the other hand, if commercial motivation is treated as an express prohibition, the number of potential litigations and ambiguity is reduced due to the clear content of the law. Commercial motivation is easier to prove based on commercial contracts and dealings, and only in the fringe cases of indirect arrangements would the factum of commercial motivation be the subject matter of litigation, which can be addressed via later rules and guidelines.

Therefore, we suggest a combination of the two approaches, similar to the model of prohibitions present in American antitrust law. This combination would involve the following

a) TMP's with commercial motivations would be illegal *per se*. **["*narrow*" approach]**
b) TMP's without commercial motivations will be assessed with respect to the "*rule of reason*", namely a reasonability assessment with respect to certain principles such as non-discrimination, proportionality etc. **["*broad*" approach]**

The following factors specific to the Indian context suggest that such an approach is desirable:

- Litigation timelines

    - ➢ As already explained above, the suggested approach reduces litigation possibilities for the category of TMP's that are sought to be prevented.
- Levels of regulation
    - ➢ The ability of a regulator to regulate network management is severely limited under a narrow approach. The only interference in a narrow approach would be to address explicitly illegal arrangements, but the regulator is constrained from intervening in order to avoid perverse incentive structures, business environments or anti-competitive effects. The prevention of these anti-competitive effects and the vitiation of the business environment serve as the primary policy reason behind this regulation. Therefore, a model of regulation that undercuts the effectiveness of the policy in addressing the need of the said regulation should not be adopted.

Question 4. If a broad regulatory approach, as suggested in Q3, is to be followed:

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?

The reasonability of a TMP may be assessed on three-fold criteria involving the following parameters

a) **Legitimate and Demonstrable Technical Need**

- Reasonability should primarily be evaluated from a *need-based approach* instead of an effects approach. This would involve making this a threshold factor in the analysis of reasonability, before the effects of the TMP are analysed using the other criteria which measure their effect.
- For example, if a TMP does not have a legitimate demonstrable technical need, it should be regarded as unreasonable per se, without an evaluation of its effects. However, where there is a legitimate demonstrable technical need, the reasonability of the TMP should be analysed with reference to its effects.
- This ensures that TMP's which do not address the problem of network congestion, and are merely attempts to either establish an incentive structure for users to pay for services, or to hide systematic underinvestment in network architecture are not allowed.

b) Narrow Tailoring

- The variation in usage patterns across networks leads to a different model of traffic, and therefore demands a different model of network management for each network.
- A reasonable TMP therefore focuses as narrowly as possible on the problem that is intended to be solved.
- There are several technical considerations that may be addressed by the narrow tailoring of a TMP to address the issue of disproportionate congestion on a network, which are
  i. Network Type
  ii. How the access nodes interact with the links
  iii. Subscriber density per access node
  iv. Backhaul network capacity.
- This could produce several models of network management which would react to the specific needs of a network based on its network architecture, and not apply generally to a broad average of a network.

c) Proportional and Reasonable Effect

- The effect of the TMP should further be measured with respect to its *effect on the end-user*, and whether this effect is reasonable or not.
- The reasonability or proportionality of these effects remains a subjective component of the test which would heavily depend on the factual analysis of each individual case. However, the broad principles of reasonable action can be imported from common law in order to guide this assessment.
- For example, it would be unreasonable to restrict a subscriber's bandwidth to 1% of the peak rate for all time just because that subscriber adds to 40% of the congestion of a network. It would however, be reasonable to reduce the priority of the traffic of the most congesting users in order to ensure quality-of-service for the large number of individual non-congesting users on the network.

Categories of traffic should not be defined by the regulator because of the different contexts of various networks. For example, a network like Reliance Jio would face greater congestion from Voice over Internet Protocol (VoIP) traffic, while other networks, for example, BSNL, which has a subscriber base largely dominated by broadband users would face different kinds of traffic, and therefore different reasons for congestion.

This has to be supplemented with a prohibition against Deep Packet Inspection by the operators. DPI presents massive risks to privacy and the freedom of the internet, and a situation where such fundamental interests of consumers can be violated by unaccountable undemocratic private bodies should not be allowed.

Therefore, there should be guidelines which delineate the *method* and *criteria* that may be used in determining categories of traffic by the operators. For eg, this could be on the basis of consumer surveys, market trends, business data and network data which can be collected without the need for DPI.

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

Application specific discrimination within a category of traffic sets up incentive structures which alter the economic environment of internet applications, and therefore, not only is it a measure of commercial intent (in situations where a particular application is granted priority or deprioritised) but also creates systems where entrenched apps with a broad user base and economic strength would be in a position to provide consumers with better services in collaboration with network operators. Given the difficulty with proving commercial intent in the absence of a contractual arrangement, this would create an unfavourable environment for newer applications, which is a principle the free internet must stand by.

b. **How should preferential treatment of particular content, activated by a users choice and without any arrangement between a TSP and content provider, be treated?**

Preferential treatment of content by user choice poses the same issues that application specific discrimination does, but with a greater magnitude. While the absence of an arrangement between a TSP and a content provider may indicate the lack of commercial intent, the consequences of allowing this preferential treatment is the setting up of similar incentive structures and business environments that prejudice new and emerging applications and businesses. The reason this business environment is worse in this instant is the lack of consumer awareness about newer apps, or a reluctance to switch to these applications. An environment where bigger applications are able to provide a better user experience, not by virtue of being a superior app, but because the market already exists for that app, it poses inherently anticompetitive consequences.

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

A narrow approach would need to have guidelines along the following lines:

a) **Transparency**

- There must be accurate and publicly accessible declarations of network management practices, the performance and terms of their services, the legitimate and demonstrable need for network management and the particular discriminations being exercised.

b) **No Blocking**

- A network provider should not be allowed to block any lawful content, application, service or non-harmful devices.

c) **Commercial Intent**

- Any network management model that is commercially motivated should be expressly prohibited for the policy reasons already outlined in the Consultation Paper, primarily in preserving the incentive structures and business environment of the Internet.

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

a) **Emergency situations and services**

The “prioritisation of emergency situations and services” should be treated as an exception on regulation of traffic. This can include situations involving the communication to emergency service providers or others necessary to make public disclosure of impending risk of disaster, emergency or public calamity. A comprehensive list of emergency services is required. These emergency services can be public calamity issues and real problems that stresses down the telecom networks. a reduced tariff can be charged in case of emergency services, subject to reporting to TRAI within seven days. For instance, the Chennai floods saw the instant mobilisation of applications targeted specifically for relief and rescue work. The national regulations could impose priority use of telecommunications infrastructure for security forces, medical personnel etc.

b) Restrictions on unlawful content

Differential treatment of traffic may be applied to fulfil the legal provisions set in the regulatory framework for electronic communications networks and services (ECNSs). In addition, court decisions can have an impact on the way ISPs and network operators deal with the management of traffic over their networks. In such cases the differentiated treatment of traffic is not at the ISP's initiative: it is forced to implement a specific treatment to comply with prescriptive court orders (normally court orders taken on the basis of some specific legislation). Some of the usual legal causes that may lead to traffic management techniques include: - blocking access to illegal use of content: in some cases, contents available through the internet can be deemed illegal and banned for public access; - copyright protection: depending on the policy on copyright protection, the availability of some contents may be restricted. The content should be in accordance with the Indian laws.

c) Maintaining security and integrity of the network

The exception of "maintaining network security and integrity of the network" is needed to avoid traffic unwanted by the users (such as viruses, spam, etc.), and preventing certain harmful or illegal activity such as the distribution of viruses or other malicious code or the transfer of child pornography or other unlawful content. To ensure that electronic communications networks run smoothly, in other words to guarantee a satisfactory quality of service, the integrity and security of public communication networks are required to be maintained.

Traffic management can also be essential to achieve and maintain network integrity. Different adverse conditions may require routine or specific traffic management techniques to be applied. Some examples of such adverse conditions and responses in terms of traffic management are: Outages: transmission or routing elements out of order. In this case, traffic management is applied for automatic traffic redirection and congestion management in order to restore minimum performance levels and/or equilibrate traffic among different elements. - External attacks: denial of service (DoS), flooding attacks or domain name system (DNS) impersonation.

This exception is necessary to prevent cyber-attacks that occur through the spread of malicious software or identity theft of end-users that occurs as a result of spyware. Typical attacks and threats that will trigger integrity and security measures include:

- flooding network components or terminal equipment with traffic to destabilise them (e.g. Denial of Service attack);
- spoofing IP addresses in order to mimic network devices or allow for unauthorised communication;
- hacking attacks against network components or terminal equipment;
- distribution of malicious software, viruses etc.

The regulatory authorities need to advance special attention to to network operators, since they are by definition the guarantors of service integrity, quality and security. They must be able to carry out adequate network management, guaranteeing compliance with obligations towards each user, in accordance with commercial supply, as long as this does not imply falling into anticompetitive or unjustly discriminatory practices.

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

A comprehensive list of services that may be notified in public interest is required in order to make this an exception.

e) Any other services

Preventing Impending Network Congestion: A sudden increase in demand for specific content, applications or services, may overflow the transmission capacity of some elements of the network and make the rest of the network less reactive. The need to apply traffic management measures going beyond the reasonable traffic management measures in order to prevent or mitigate the effects of temporary or exceptional network congestion should not give providers of internet access services the possibility to circumvent the general prohibition on blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services, or specific categories thereof.

In general, congestion can have two causes: unpredictable situations that occur on an irregular basis (such as statistical fluctuations of traffic flows or fault conditions within the network) or relatively predicable situations occurring at a regular basis (because of failure to increase the capacity of the network according to the growing traffic load). Congestion may result in high latency, packet loss or blocking of new connections, with potential impact on service availability and on the users' experience.

Question 7. How should the following practices be defined and what are the tests, thresh- olds and technical tools that can be adopted to detect their deployment?

a) Blocking

The US Open Order 2015 states that no blocking is allowed. "A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management."

The concept of open internet is essentially based on the idea that no lawful content or non-harmful device can be blocked from the internet. TRAI should enforce a no-blocking requirement for both incoming and outgoing traffic. This should be subject to the exceptions identified under reasonable traffic management. In all other situations, blocking of content should only be possible under a direction under Section 69A or 79 of the Information Technology Act. Networks may block devices that do not comply with industry established standards if they have the potential to affect the security and stability of the network.

b) Throttling

The US Open Order states that No throttling is allowed. "A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management."

The US Open Order report of 2010 recognises that "in some circumstances the distinction between blocking and degrading (such as by delaying) traffic is merely semantic."

The Netherlands law for net neutrality states that "Providers of public electronic communications networks via which Internet access services are delivered and providers of Internet access services shall not hinder or slow down applications or services on the Internet."

As per EU, throttling includes "Slow down, alter, restrict, interfere with, degrade or discriminate".

Throttling is equivalent to blocking since the effective consumption of a service would be reduced if its quality of service is degraded. Rules for throttling should be similar to blocking.

Throttling should be allowed to deal with the situations identified in reasonable traffic management.

c) Preferential Treatment

The US open order 2015 states that paid prioritisation should be banned. “A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not engage in paid prioritization.”

Paid prioritization defined according to US open order “refers to the management of a broadband provider’s network to directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either (a) in exchange for consideration (monetary or otherwise) from a third party, or (b) to benefit an affiliated entity.”

The rules should be formed by TRAI to treat broadband service like a public utility and prevent internet service providers from offering preferential treatment to sites that pay for faster service. These rules should be formed in a way to prevent service providers from charging higher traffic management prices to Web services that they see as competitors. The service providers should not be able to impose a new price of entry for innovation on the internet.

Question 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?

Identification of net neutrality violations become a lot easier if the asymmetry of the information is corrected. The Over the Top Service Providers, in the accessibility of technical information, will be able to provide better services and shall hence boost confidence of the consumer and regulator’s effectiveness. With respect to what should be disclosed, it is submitted that all information that will be relevant for making an informed choice by the consumer and for regulation purposes by the regulator must be made available in an accessible format, other than that which will affect stability and network security.

It is recommended that a combination of the above be adopted for ensuring transparency *in toto*. For analyzing the extent to which the TSPs are meeting the guidelines proposed, disclosures should be put up on the website of the concerned TSP. This should contain all the relevant information that can be used by consumers, government agencies and the civil society as a whole for choosing the service provider, which is most conducive to their preferences. The website must be updated regularly with such information, as and when there is any substantial change. Since this is difficult to regulate, a yearly update must be made mandatory.

Other than disclosures to the public, it is submitted that filings to TRAI need to be made by these service providers in a technically substantial manner at regular intervals, where time lapsed between each submission should not be greater than half a year. These should be detailed and furnishing general and specific metrics (like Operations Support Systems and Business Support Systems).

Question 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]

Substantial changes to the template are not necessary as such. Relevant aspects like Pricing Option, Performance Details, Service Limitation and Traffic Management, Application Agnostic Traffic Management, User Triggered Traffic Management have been covered. The answer to Q.8 need be referred to where requisites for a full and empowering disclosure are discussed.

A varying document for each stakeholder may *not* be necessary if the TSP makes available all the relevant documents on its website.

Question 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?

In the last few decades, Internet has become a very indispensable part of our lives being regarded as a medium for open, unrestricted and free exchange of information. There is a legitimate expectation stemming from the user of the Internet that it should be open and neutral and this architectural character is considered to be the main motivating force behind the unparallel success that has been achieved by Internet and to create an ecosystem which has been conducive to the boom witnessed in proliferating of online applications, content and services.[2]

The diversity of the services offered via Internet, the popularity of broadband Internet services, and the bundling of services by service providers, all create an incentive for ISPs to interpret the ‘best effort’ principle in a liberal, or to even abandon the principle altogether. ISPs can now incur financial and efficiency advantages by indulging in “vertical integration” of the production, editing, and delivery of content.[3] The step towards involvement in active management of content results not from an affirmative obligation to do so, but instead the desire to tap new business opportunities accruing from the ability to scrutinize bitstreams.[4] Such scrutiny can facilitate the prioritization of traffic into tiers corresponding to different quality of service commitments.[5] The advent of paid prioritization arrangements between big companies and service providers are going to be the result of these traffic management techniques.

Adoption of clear transparency standards and Quality of Service (Qos) are some of the methods that can be employed to prevent service providers from imposing unreasonable restrictions on the provision of Internet access. At the same time, the regulator/concerned authorities need to decide on a practical, feasible and appropriate scope for the term ‘neutrality’, since this principle is applicable not only with regards to access and accessibility, but also with general or inconsequential alteration with speed or relative quality of Internet services. Since Net Neutrality is a multi dimensional concept, one of the likely outcome of over regulation vis-a-vis further evolution of technology is that it could lead to over complication and expensive solution to a problem that might not warrant such regulation. The principles of net neutrality have to be made flexible and periodic reviews are the need of the hour. A more collaborative approach involving multiple stake holders has to be embraced by TRAI.

[2] Sietse van der Gaast*, Net neutrality observed in more detail: Influences on end user experienced neutrality of Internet based services, available at* http://www.stratix.nl/academy/publicaties/netneutraliteit_cnri_sietse_nov2010.pdf.

[3] Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers,* Vol. 18(3) FORDHAM INTELLECTUAL PROPERTY, MEDIA AND ENTERTAINMENT LAW JOURNAL, 634, 636, (2008).

[4] *Ibid.*

[5] *Ibid.*

Question14. 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.

The quality of internet may be adversely affected by factors beyond the ISP, resulting in degradation of internet services. The internet speed may vary due to hardware or network equipment or processors. However, this does not affect the speed of connection received from the ISP. In the context of Net Neutrality, these can be taken into consideration by providing *minimum* quality of service requirements as a reasonable discrimination. QoS must improve transparency.[6] The ISP should provide sufficient information to ensure that *all* end-users are aware of the minimum quality of service and any other parameters affecting the quality. It should provide information about any restrictions or conditions which limit access to internet services or individual applications. Thus, the end-user can monitor his/her internet access service.

Monitoring of quality would impose a higher burden. The primary question which arises is whether there is a need for regulatory intervention. In the EU, Article 22(3) of the Universal Service Directive itself does not provide concrete criteria to assess when this need arises. The BEREC Guidelines suggest two different regulatory approaches – proactive and reactive. In the Indian context, we could use a mixed-model approach which could receive proactively monitor whether minimum QoS are met, and reactively accept complaints from the stakeholders and decide ad-hoc whether regulatory intervention is needed.

[6] Body of European Regulators for Electronic Communications, *BEREC Guidelines for quality of service in the scope of net neutrality* (2012).