Unearthing the impact
of the Internet on democracy
in India and beyond

www.internetdemocracy.in

internet
democracy
project

12 April 2017

To,
Shri Asit Kadayan,
Advisor (QoS)
Telecom Regulatory Authority of India,
New Delhi

Dear Sir/Madam,

Thank you for the opportunity to comment on the consultation paper on net neutrality. Please find below the response from Internet Democracy Project (https://internetdemocracy.in) to the consultation paper.

The Internet Democracy Project is a Delhi-based civil society initiative that works for an Internet that supports freedom of expression, democracy and social justice through research, advocacy and debate in India, and beyond.

Please do let us know if you need any further clarifications regarding our submission. We hope that our comments will be taken into consideration.

Thank you and best regards,
For the Internet Democracy Project,

Nayantara

Nayantara Ranganathan
Programme Manager- Freedom of Expression
Internet Democracy Project

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

In our submission to the pre-consultation paper, we cited the principles listed by Barbara van Schewick in 'Network Neutrality and Quality of Service: What should a non-discrimination rule look like?'[1] as key points that any net neutrality framework should seek to preserve in the Indian context. We reiterate that these are useful characteristics that make the internet a medium of unprecedented value and reach, and TRAI should keep them in mind in expanding on the meaning of 'non-discriminatory access'. TRAI itself named three of the four principles as important in the pre-consultation paper, excluding 'application blindness of the network'. Excluding application blindness of the network can be especially damaging in the Indian telecom context, as TSPs are incentivised to discriminate against some classes of applications. In the past, TSPs have had issues with entire classes of applications like VoIP, which allegedly cannibalise their revenues, and TMP provide a good front. We urged TRAI to consider the four together, as it is intended:

- User choice
- Innovation without permission
- Application blindness of the network
- Low costs of application innovation

TRAI contemplates the approaches that countries have taken and finds that the Indian approach to ensuring non-discriminatory access can be one of two routes- (a) articulating 'brightline' rules and qualifying it with a reasonable traffic management and (b) laying down principles of network neutrality and clarifying that this will not prevent reasonable management of networks.

'Reasonable' network management should be defined in the former approach, demarcating exceptions as opposed to simply stating that traffic management will be allowed. The broader approach is preferred. Content providers as well as telecom service providers are looking for certainty about what they can invest in, what is disallowed etc. With a thriving start-up sector innovating in applications and a growing Internet user base, TRAI should actively articulate bright-line rules, instead of going for the second approach.

TMPs are a potent way for TSPs to circumvent non-discriminatory access to the internet and do what is not allowed otherwise: favour some applications (or types of applications) over others.

[1] See http://cyberlaw.stanford.edu/downloads/20120611-NetworkNeutrality.pdf

It becomes important therefore to limit TSPs' ability to make use of TMP as a front for discrimination, by taking the first approach, and defining what is 'reasonable' traffic management.

Question 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.

The Dynamic Coalition on Net Neutrality defines specialised services as '*electronic communications services that are provided and operated within closed electronic communications networks using the Internet Protocol, but not being a part of the Internet. The expression "closed electronic communications networks" refers to networks that rely on strict admission control.*'[2] Provision of such network services using closed electronic communications networks, thus, should be on separate infrastructure. If it does connect to all end-points on the internet, then the service should not be classified as a specialised service, as it would sacrifice the bandwidth available for internet services.

The scope of 'Internet Services' should encompass all the end-points in the global information system linked together by unique IP addresses and supporting TCP/IP suite or IP compatible protocols, as opposed to consumption for a 'predetermined set of end users' (Body of European Regulators for Electronic Communications (BEREC) Guidelines, 2016[3]). If the network is intended to serve only a subset of users who use IP-based protocols for networking, then such a network should not be part of 'internet services'.

To ensure that TSPs do not subvert compliance of non-discriminatory access by offering a service as a specialised service, it is important to assess whether such a service could not have been provided over the public internet. The BEREC guidelines also warns about this:

[2] See https://www.slideshare.net/FGV-Brazil/net-neutrality-reloaded-zero-rating-specialised-service-ad-blocking-and-traffic-management

[3] See http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6075-draft-berec-guidelines-on-implementation_0.pdf

> NRAs (National Regulatory Authorities) should verify whether, and to what extent, optimised delivery is objectively necessary to ensure one or more specific and key features of the applications, and to enable a corresponding quality assurance to be given to end-users. To do this, the NRA should assess whether an electronic communication service, other than IAS (Internet Access Services), requires a level of quality that cannot be assured over a IAS. If not, these electronic communication services are likely to circumvent the provisions of the Regulation and are therefore not allowed.

On the specific services mentioned in the question:

Virtual Private Networks (VPNs): VPNs, insofar as they provide access to a limited number of end-points on the internet, the way some corporate actors do, can qualify as a specialised service. But a VPN service that provides access to the public internet without restrictions should not be classified as a specialised service, as it gives access to all end-points on the internet. As the consultation paper points out, the BEREC guidelines also follow this approach of classifying VPNs that connect to the internet to be within the scope of the EU regulations.

Content Distribution Networks (CDNs): Some content providers are capable of buying CDN space and hosting their content closer to the edges, while smaller players are not. The operative part is whether any content provider is being precluded from making such arrangements with TSPs. Since deploying high traffic content closer to the edges eases up the load on the network as a whole, it need not be treated as violating discriminatory access to the internet. However, there is a needs to be transparency in these peering arrangements, so that some application providers are not denied interconnection arbitrarily.

Internet of Things (IoT): Internet of Things should **not** be an exception to net neutrality.

Connectivity to the Internet is integral to the success of Internet of Things. Management and analysis of data is often done in the cloud, and the devices are connected to smartphones. The expectation in the use of IoT devices is that the service will have high and reliable speeds. But prioritising these services would be at the expense of the general-purpose internet, sacrificing bandwidth available for free usage, violating non-discriminatory access to content, applications and services on the Internet. However, customers who are willing to prioritise their IoT-enabled devices within their own bandwidth caps should be allowed to do so with user-controlled QoS[4] or use it as a specialised service.

[4] User-controlled QoS in 'Network neutrality and Quality of Service: What should a non-discrimination rule look like?' is qualified by the following conditions:

(1) the different classes of service are offered equally to all applications and classes of applications;

(2) the user is able to choose whether and when to use which class of service;

Question 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.

As the TRAI paper notes, a principle-based approach (the broad approach) would make the regulations applicable even in the face of technologies that would come up in the future. This would provide much needed flexibility, as the prospective monitoring and enforcement body would have a touchstone from which to assess whether a particular TMP is harmful or not.

Question 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?

The comments of the EU Council of Ministers Committee on Net Neutrality is worth going back to in this context: '*exceptions to this principle should be considered with great circumspection and need to be justified by overriding public interests*'.[5]

TMPs should be regarded as reasonable if all of the following considerations are met:

A. It is not carried out as a result of a commercial arrangement, with or without money as consideration.
   As the consultation points out, all jurisdictions that have adopted network neutrality policy frameworks consider TMP driven by business arrangements or incentives as discriminatory.

(3) the network provider is allowed to charge only its own Internet service customers for the use of the different classes of service.

[5] See http://archive1.diplomacy.edu/pool/fileInline.php?IDPool=1204

B. There should be no discrimination between applications of the same type or between classes of applications. Discrimination between classes of application should not be considered reasonable unless it was the last resort. Even then, the TSP should be able to provide justification in their periodic reporting of TMP used.

   Allowing discrimination among classes of applications because they have different characteristics is not as harmless as it seems. Network operators are incentivised to favour one type of application over another. In the Indian scenario, TSPs are dead against VoIP services on the internet, for example. Barbara van Schewick makes a case in great detail about why allowing discrimination between classes of applications is harmful. In short, she emphasises how it is in various groups' interests to disincentivise some classes of applications over others- discriminating against peer-to-peer file-sharing applications for example.

C. Such a user activated QoS should be allowed, as long as users are privileging particular content or application within their own bandwidth caps.

   TSPs should not be deciding QoS for different applications on its own. Preferential treatment of certain applications, activated by the user should be allowed, as it increases user choice. However, such an option should be available for all users and any application or content provider should be able to offer their content/service in optimised manner.

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

As mentioned in the TRAI consultation paper, a narrow approach can only bring certainty for technologies in existence today. Given that use-cases of the internet and associated networks are ever-changing, along with the network equipment technology used for TMP, a narrow approach would get outdated in no time. TRAI also brings attention to other pitfalls of a narrow approach- lack of a commercial motivation does not mean a TMP is harmless, and foreseeable harms are mostly commercially motivated. Besides, commercial motivations are not only of the monetary or contractual kind, and can be hard to identify.

For these reasons, a narrow approach is not suited for a net neutrality framework in India.

Exceptions to regulation

Question 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.

a) **Emergency services**: It is not clear how services would be identified- whether on the basis of origin and destination of traffic, whether it is limited by time, and the question of who decides whether a situation merits classification as an emergency. It is understandable that the definition cannot be hard-coded and might have to adapt to ad-hoc situations that emergencies like natural disasters throw up. However, the scope of these services should be narrow, such that any situation should not be classified as an emergency. This has been seen in the use of section 144 to shut down internet services. TRAI should guard against such misuse.

- In a previous consultation paper on emergency services, two broad types of issues emerge when it comes to disaster recovery and response

  (a) loss of infrastructure, including physical destruction of network components and disruption in supporting network infrastructure
  (b) Overload/Network Congestion

  Only the second type of issue can be addressed in creating an exception for non-discrimination rules.

- Further, a comment in a previous consultation paper on the scale of the disaster is useful:

> While some of the emergency situations may be highly localized, others may spread over large geographical locations. Some of the situations may result in transient network outages for a short duration, others may require prolonged state of relief and rescue spread over a large geographical location. The different situations warrant different approaches and hence a classification of failure of telecommunication during emergency/disaster is must. The size/nature of the disaster is not the determining factor of the effect on telecom infrastructure; rather it's how the destruction affects the facilities/network for communications.

Determination of when a situation is a ‘disaster’ is subjective, as are approaches to be used in such situations. Therefore, it is important to ensure that there are checks and balances in making a determination about whether the situation is an emergency, and if so whether telecommunication networks have been affected, and narrowly tailor the response.

Considerations such as the following on temporality are useful in designing the appropriate response:

> One of the stakeholders has opined out that Loss of infrastructure and Overload/Network congestion pose different challenges when they occur individually and together depending on the nature of emergency/disaster. For example priority call routing may not address leadership communication requirements in case of loss of infrastructure, particularly in the crucial initial stages. [...] Priority call routing cannot serve as the mainstay of first responder communications. ‘Fairness’ of the concept lies in the fact that, as the emergency extends in the time dimension two things are happening (a) the first responder radio network has stabilized and the satellite–based Emergency Communication assets of the Disaster Management agencies have been rolled out (b) the Mobile Service Provider has restored and temporarily augment local communication capacity; otherwise priority routing will deprive the calling from subscribers, whose own requirements to communicate are peaking as the duration of emergency extends in time.

b) **Restrictions on unlawful content**: Restrictions on unlawful content should not be an exception to network neutrality. Mechanisms to address unlawful content is present under the IT Act. This is sufficient. In order to ensure that TSPs are only blocking such content as is mandated by orders under the IT Act, TRAI should recommend to the DoT to make all such orders transparent to the public.

c) **Maintaining security and integrity of the network**: While it is challenging to comprehensively list out what would come under the definition of ‘security and integrity’ of the network, not listing any would be liable to misuse. BEREC also had similar concerns about ‘security’ being a broad concept. A number of TMP applied at various layers can be towards maintaining security and integrity of the network. However, some practices are more intrusive than others. It should be proved that the measure undertaken is directly related to the stated goal, and that the measure is the least intrusive way of handling the issue.

d) **Government notified content**: No, government notified content should not be an exception to network neutrality. Government notified content should not be treated any differently from content by any other actor. This will lead to a very patronistic access, undermining user choice and application blindness of the network.

Government-mandated or endorsed content/applications/services need not always be the most useful choice for the user. Such a prioritisation still shapes user preferences in many ways, disadvantaging other content/applications/services in the market.

Question 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?).

Blocking: TSPs should not block any application, content or service based on the end-user, the content provider, the protocols, the type of application, or the content of application. TRAI should recommend to the DoT that blocking orders under the IT Act should be made transparent, so that it is easy to distinguish between an instance of blocking because of orders under the IT Act or a violation of network neutrality.

Throttling and preferential treatment: With regards to throttling and preferential treatment, TRAI should use a variety of measures to determine if there are violations happening. The primary measure should be requiring detailed disclosure on technologies being used to positively or negatively discriminate for traffic management purposes. Such disclosures should happen regularly and these practices should be audited regularly. This should be supplemented with structured network measurement tests conducted by TRAI, with open tools like OONI and M-Lab which are available. TRAI should explore facilitation of such tests by users through portals for the purpose, in the way that TRAI has created a QoS portal, or the MySpeed portal. TRAI should also have a grievance redressal system, where consumers - whether end users of applications or developers and creators - can come in with complaints also.

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?

Option (d), a combination of disclosures to consumers, to the regulator and to the public is preferred.

To the general public, disclosures should be made in an easily accessible manner to consumers at the point of sale and on the website of the TSPs, similar to the way that price information is mandated to be disclosed. This information should include the TMP that is used, trends that have been observed about the time/situations in which certain TMP have to be deployed what it means for the use and access of certain types of content/applications/services.

To the regulator, TSPs should disclose in detail the TMP used for different kinds of issues upfront, and also periodically submit details of instances where TMP had to be employed, and reasons for the same. The regulator should also be able to inquire into TMP undertaken during certain periods taking cognisance of issues from complaints submitted by users or suo-moto.

To general public and customers, the Telecom Tariff Orders have some characteristics which are also useful to adapt in case of reporting of TMPs.

- Information in vernacular language also
- Prescribing a minimum font size for the physical printed material
- Provide instances of traffic management that was carried out in the period of billing
- Colour code the different types of effects that such traffic management practices can have
- Let both prepaid and postpaid users know as and when traffic management techniques are activated for the duration that it is being deployed

We reiterate the points in our submission to the pre-consultation:

> TRAI should put in place transparency requirements in the license agreements mandating that all service providers disclose consistently traffic management tools that are available with them, the exceptional situations in which they are used, and the effect of that use, and that they do so without a prior complaint, in a systematic manner. Conversely, it should also be true that any traffic management practice that is not disclosed, even when used for legitimate exceptional cases of network congestion would be liable to penalties.
>
> This is fairly consistent practice in several network neutrality regulations that cover traffic management. For example, disclosure of such practices is one of the factors used to evaluate the ‘reasonableness’ of traffic management in the Open Internet Order passed by the Federal Communications Commission. Specifically, the Order requires a broadband provider to ‘publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device

providers to develop, market, and maintain Internet offerings.' (https://www.law.cornell.edu/cfr/text/47/8.3)

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]

For the purposes of displaying on the website of TSPs, the table can be used. However, disclosures to the regulator should be disaggregated by date, applications (where there has been throttling or prioritisation on the basis of classes of applications). Even information aimed at customers should be required to be provided in regional languages and made accessible and comparable using colour schemes.

Question 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?

TRAI should be responsible for monitoring and supervision, under its powers of regulating on the subject of Quality of Service. Section 11 of the TRAI Act also gives TRAI sufficient jurisdiction for ensuring compliance of license terms by service providers, so TRAI can also be involved in monitoring for compliance if the license conditions are amended to include a requirement to follow network neutrality regulations laid down by TRAI. In case of detected violations, TRAI should be empowered to impose penalties.

Our recommendations therefore are:
A: TRAI regulate on issues of traffic management under its mandate to set QoS standards. TRAI should investigate complaints and make suo-moto inquiries about traffic management practices.
B: TRAI recommend that DoT amend license conditions to impose a requirement for complying with net neutrality regulations that TRAI puts in place.

Question 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).

a) Ensuring that information being disclosed by telecom companies is correct is a challenge. However, correlating network measurements conducted by independent bodies and consumer complaints and patterns established in them, the veracity of information disclosed can be ascertained to an extent
b) Load of complaints could be high
c) Issues could go undetected by customers, because of the limited availability of information. For this reason, consumer complaints cannot replace detailed disclosure by TSPs
d) It is hard for third parties to get access to information held by TSPs, especially contractual information. TRAI should be empowered to look into interconnection agreements and other contracts between ISPs, so that action regarding violations can be proactive as opposed to reactive

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?

Yes, having a multi-stakeholder mechanism can complement TRAI in some operational aspects of the network neutrality framework. The authority can help in convening the meetings and identifying stakeholder groups.

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? [See Chapter 6]

Having multi-stakeholder inputs complementing the monitoring of network neutrality violations ensures that there is more capacity for identifying new technologies and use cases that haven’t been considered.

A principle-based approach would be another way to ensure that the framework is future-proof. Not making policies with specific technologies in mind is a classic way of ensuring that the policies remain relevant in the face of advancement, and should be the way forward for a network neutrality framework as well.

Question 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]

Difference in experience stemming from the use of different end-user devices or softwares should not be a concern for net neutrality debates. Net neutrality seeks to ensure that the service providers provide non-discriminatory access. A difference in experience has existed, and has been an element ever since the internet has existed. The internet has also adapted to such varied user experience- take for example how the world wide web has adapted to mobile, and is getting better. However, for the internet to remain the valuable resource that it is, and continue to be a democratic force for political, economic, social and cultural gains, ensuring a non-discriminatory access to networks is of utmost importance.