

Response to TRAI
Pre Consultation Paper on
Net Neutrality

July 2016

Pre- Consultation Paper on Net Neutrality

NASSCOM and its members firmly believe that net neutrality is a core to the future of the India's digital economy and that the Government must implement adequate safeguards to ensure that principles of net neutrality are preserved, and ensuring that no new hurdles are created that could potentially stifle the innovative digital ecosystem like OTT services.

Therefore, interventions being contemplated by TRAI should be guided by the broader objectives of promoting innovation and universal connectivity for all Indians, without compromising on the principles of net neutrality.

Our responses to the specific questions are as follows:

1) What should be regarded as the core principles of net neutrality in the Indian context? What are the key issues that are required to be considered so that the principles of net neutrality are ensured?

Net Neutrality is a universal concept¹ (recently upheld by US courts as well as other nations in the past) where TSPs, as access providers, have no power to influence consumer choice relating to services, applications, content that a consumer accesses. The consumers retain their Right to select, and make informed decision on how to use their Internet access offered by the TSPs.

Net Neutrality therefore, should ensure unrestrained access to content and services once the user has subscribed to data services, subject to National regulations related to security and privacy.

Upholding principles of Net neutrality will ensure that developers continue to innovate and that consumers retain their right to select services that compete on features and price, and make informed decision on how to use their Internet access offered by the TSPs. This principle is essential to ensure that TSPs are not permitted to distort competitive forces by leveraging their exclusive control over access infrastructure.

¹ http://www.nytimes.com/2016/06/15/technology/net-neutrality-fcc-appeals-court-ruling.html?_r=0

Net Neutrality in our view should be characterized by the following attributes

- 1** User to have the unfettered right of making an informed choice in deciding content / services to access
 - 2** No discretion to TSPs to censor or block access to any legal content, applications, services, or non-harmful devices or determine how users use internet
 - 3** No right of TSPs to throttle lawful internet traffic on the basis of content, applications, services or non-harmful devices. In fact, opening of the content of transmissions other than when required under laid down legal processes, is illegal.
 - 4** No right of TSPs to speed-up / favour lawful internet traffic over other lawful traffic in exchange for consideration of any kind²
 - 5** Critical that there be a level playing field for all Internet platforms and services including particularly entrepreneurial start-ups so that they are not squeezed out by either TSPs or large/global Internet Platforms and Service providers through anti-competitive tie-ups or practices
 - 6** Prioritization of Emergency or any other services as prescribed by the regulator accompanied by public declaration and without price discrimination
 - 7** Clear and declared definition of acceptable technical practices by TSPs for management of network traffic in conformity with above principles
 - 8** No double dipping by Telecom Service Providers. Charges would be levied only from end customers based on data consumption and not from Internet Platforms and Applications
 - 9** Security restrictions as required for ensuring reliable services and lawful demand of security agencies.
-

The framework above should be implemented keeping in mind the broader underlying objective of promoting universal connectivity and enhancing internet penetration at a time when more than one billion Indians are without connectivity. This requires TRAI to work actively to facilitate innovation and dissolve barriers to entry.

² Commercial or non-commercial gains

2) What are the reasonable traffic management practices that may need to be followed by TSPs while providing Internet access services and in what manner could these be misused? Are there any other current or potential practices in India that may give rise to concerns about net neutrality?

Principle of Net neutrality does not prevent traffic management practices that are consistent and have an enforceable framework to make sure such practices are reasonable, i.e. situations under which they are warranted and mechanism adopted e.g.

- Unforeseeable transitory congestion - maybe due to equipment failure or other reasons, may require traffic optimization measures. However, operators must be able to prove that such congestion of its network was not foreseeable and that it took necessary steps to correct it.
 - Security threat from a sudden attack, malicious actions aiming at altering the global operation of the network, whether intentional or accidental.
 - Prioritization for stipulated emergency services only, that have been declared publicly in the larger public interest, ensuring no discrimination among Internet Platform and service providers of the same category.
-

Therefore, beyond the needs of optimizing the network and addressing traffic hazards through temporary measures, either manually or automatically, no discrimination should be permitted. They should not directly and indirectly bring in any discrimination – price based/ non –price based.

As per the FCC open Internet Order, 2015,

A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service.³

We strongly recommend that from a legislation point of view, there should not be any preference for one network technology over another, since it may lead to market distortions. At the same time, TRAI must ensure that innovation is allowed to flourish

³ https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

by instituting a flexible and light-touch approach which facilitates innovation in models, technology, and business agreements.

Traffic management practices that are reasonable and consistent should be implemented in a transparent manner. This will require audits and scrutiny as well as safeguards and penalties to prevent misuse, and full disclosure to the regulator would be essential. Making available traffic management policies and sharing information on how telecom services are affected by traffic management with the users is important and necessary.

3) What should be India's policy and/or regulatory approach in dealing with issues relating to net neutrality? Please comment with justifications.

The regulatory framework should incorporate suitable provisions to ensure net neutrality is maintained, and that there are appropriate enforcement mechanisms to deal with any complaints or reported breach of the principles. As consumers increasingly rely on the Internet and Mobile networks for not only their communication needs, but other needs like Banking, transportation, Health etc., we believe that the attributes as listed in response to Q 1 of open and fair access should be upheld and any violation of these principles should be critically examined and actioned against.

Universal principles of net neutrality, access for all and leveraging Internet for development, growth should be upheld within the regulatory framework of Telecom Service Providers. There should be no roadblocks to rapid adoption of ICT enabled models expected to drive the Digital revolution in the country.

This is essential for a sustainable and healthy growth of a knowledge based economy, where there is a level playing field for new emerging companies, as they develop innovation led technology driven products and services.

Anti-Net neutrality practices are thus fundamentally anti-competitive and harm consumers as well as economic growth. They discourage innovation and result in rent-seeking behaviors from established players.

4) What precautions must be taken with respect to the activities of TSPs and content providers to ensure that national security interests are preserved? Please comment with justification.

From national security viewpoint, law of the land should be enforceable on all service providers and content providers who are providing services in India and be subjected to the territorial jurisdiction of India. Telecom sector is considered as Critical Infrastructure of the economy. National security risks in the form of espionage, sabotage, and foreign interference can arise in the global supply chain for telecommunications equipment, services, or the outsourcing of sensitive network management functions. It is vital that these security risks are managed to protect the availability and integrity of telecommunications networks and systems and the confidentiality of information stored and carried on these networks and systems.

There is no denying that concerns especially those relating to national security are genuine and important, and must be respected by all TSPs and Content Providers. Globally, Government data that are critical and sensitive from a national security perspective, are typically located within their territory. However private sector in general should not be subjected to such restrictions.

At the same time, companies are obliged to support Law Enforcement Agencies (LEAs) of different countries in crime investigations (access to data records, evidence) and forensics. The support should be transparent and timely, respecting the laws of the country from where request has originated, irrespective of the location of the data storage.

While many of these issues and concerns need global discussions and solutions, any knee-jerk reaction of governments which favours data localization / regulation of content providers will be a matter of great concern. Subjecting content providers to the requirements of data/infrastructure localization in name of national security will prove to be counterproductive for variety of reasons including:

- Localization requirements prohibits organizations from achieving economies of scale and leveraging global sourcing hyperspecialization benefits, resulting in increasing cost of services that could be passed on to consumers
- It threaten major new advances in technology and innovation
- It threaten open architecture of the Internet
- If similar policy directions are followed by other countries, it will severely hit established Indian IT-BPM industry sector including the emerging cloud industry which is major contributor to the Indian GDP

To overcome the challenges identified above, Government should work with the other nations in plurilateral, multilateral and bilateral forums to discuss and come out with solutions. In the age of Internet, global cooperation is quintessential and therefore India should take leadership in identified forums to ensure that its issues are addressed.

Also, Indian LEAs should also be effectively resourced and trained to raise legal requests for gaining lawful access to data from TSPs/ ISPs and content providers through the MLAT route. Further, there is also a dire need to improve procedures and frameworks for data sought by LEAs from Content Service Providers both in India and abroad. This can be done by establishing institutional frameworks possibly by establishing nodal agencies for seeking such information and standardizing disclosure norms across the service providers, and mandating all LEAs to follow well defined processes.

5) What precautions must be taken with respect to the activities of TSPs and content providers to maintain customer privacy? Please comment with justification.

Maintaining privacy of citizens has always been a concern for the nation states, and has grown more after revelations of mass surveillance by a few nation states, and increasing instance of cybercrimes, unauthorized access and espionage of data. This approach can increasingly be seen with the various countries around the globe enacting or amending privacy laws, regulations and data flow arrangements.

In India, in absence of a comprehensive privacy or data protection law, such requirements are addressed through patchwork of legislations and regulations. Some of the aspects have been built in Section 43A and rules notified under it, and Section 72, 72A of the Information Technology (Amendment) Act, 2008.

Sec 43A rules require Body Corporates (as defined in the rules) to maintain Reasonable Security Practices and Procedures to protect Sensitive Personal Data or Information (as defined in the rules). It requires them to publish a detailed privacy policy that is applicable to all users on their website, collect only that data which is essential for providing services, specify the purpose for data processing, whether it will be shared/ transferred, retention and further use, reasonable security practices and procedures to be adhered to etc. Although privacy principles are not explicitly written as principles, they can be derived from the rules. Section 72A entails criminal liability provisions for sharing personal information in breach of a lawful contract. Additionally, India has Aadhaar (Targeted Delivery of Financial and other Subsidies,

benefits and services) Act, 2016, Consumer protection laws, sectoral regulations that have elements of privacy protection.

TSPs and Content service providers (mostly Data Controllers) too are liable to protect against personal data misuse. They not only include websites and portals, but also mobile applications providing specific functionalities and services in exchange of personal information. They are required to address privacy concerns that arise while collecting, storing, processing and transferring PI. Content providers usually use TSP/ISP services as a medium to provide services to customers. All of the players involved in data lifecycle and having access to PI should be covered under content provider's privacy program for maintaining privacy of the customers.

Usually, organizations have a privacy policy in place to ensure safety, security and privacy of the users, and this is made available to the users through the terms and conditions. For any Internet Platforms and Services to even survive and compete, they have to abide by global standards and expectations. There is a strong user led review mechanism that help users rate and choose the Internet Platforms and Services. Further content rating systems are relied on by stores such as Apple, Google and Microsoft, which further ensure best practices and minimum standards where users champion apps in a democratic fashion.

There is a continuous effort on the part of start-ups and businesses to plug holes, and develop better protection mechanisms like App stores for kids, parental control, anti-virus / phishing tools that contribute towards enhancing safety and privacy of users on the internet.

Much work has already been done with respect to development of privacy framework by Justice AP Shah Committee for framing a Privacy legislation. A much needed Privacy legislation in India should be lightweight, and should allow self-regulatory apparatus to function. The legislation should list down privacy principles to be followed, scope and applicability, enforcement mechanisms, grievance redressal and recourse mechanism amongst others. Legislation should advocate use of international standards and guidelines (without going into specifics), for making privacy practices inherent part of process and technology design. Incorporation of privacy aspects should be market driven, with practices and procedures evolved from global best practices.

6) What further issues should be considered for a comprehensive policy framework for defining the relationship between TSPs and OTT content providers?

As outlined in the attributes of net neutrality, relationship between OTT content providers and TSPs is directly with the customer, with each offering different functionalities

- TSPs offer network infrastructure and services
- OTT services provide application layer services.

Therefore, any approach towards net neutrality will govern the relationship between TSPs, ISP and the users. Any relation between TSP and OTTs should under no circumstances compromise on free and open access to internet as net neutrality requires the Internet to not favour any app/site/service over others.

The belief that it is OTTs ride over the top of telecom networks and therefore need a framework for defining relationship is misplaced. Consumers use telecom networks to access apps and internet platforms. These consumers have contracts with telecom companies and they are using bandwidth that they have paid for at a price that generates profit for telecom companies.

Today there are already adequate laws controlling their operations under the IT Act, not to mention the conventional IPC, CrPC, etc. In fact, as the consultation paper itself points out, TRAI has no jurisdiction over non-communication service providing Internet Platforms and Applications.

The only issues that need to be addressed therefore, are the regulations needed to ensure that TSPs do not resort to market distorting practices which go against the principles of Net Neutrality.

There is absolutely no need from a logical point of view and no practicability from a technology point of view of bringing in TRAI regulations/ controls on OTTs

Any stifling regulations applicable to OTTs may

Create significant difficulty for business

Seriously hamper the growth and success of the start-up and SME companies

Limit the scope and potential of the ecosystem that needs to rapidly develop and adopt Innovative ICT technologies, products and services to meet India's needs and the lofty vision of Digital India

Further, there is no basis for differentiating between communications services and internet platforms offering communication services and other services. Various apps incorporate communication as a part of their offering. For example, a classified site or app may offer the buyer a feature of sending a message to the seller and even though communication is not the primary purpose of the app it is an integral part.