

Response to TRAI
Pre-Consultation on Net Neutrality

4th July, 2016

Rajeev Chandrasekhar
Member of Parliament

A. PREAMBLE: THE NET NEUTRALITY DEBATE IN INDIA

Over the past 18 months, there have been some efforts to characterize Net Neutrality as an issue of Philosophy or something complex or utopian – It is in fact none of these. It is a real issue, it is simple to understand, it is simple to define, legislate and regulate for and is core Consumer Interest issue and to preserving the character of the Internet as it is today - which is fair, open, innovative, growing

The following are the basic principles for a discussion on regulations and policies for the Internet and Net Neutrality:

- i. Internet is a global network of computer networks - consisting of millions of servers and machines interconnected through a complex mesh of gateways and root servers etc. It has no owner and there is no entity that controls access to it. That is the essential character of the Internet. It must remain that way. The defining values of the Internet are its neutrality to content and participants. It is fair and open. It has no owners and no control.
- ii. The Internet is an open collaborative platform that has revolutionized the modern world as we know it today – it is about innovation and on it and in it resides the leading innovations of today's modern world. It has thrown up and is throwing up and will continue to throw up millions of innovative applications, services and content – all of which are the legitimate right of an Internet user to access. The only exceptions are restrictions of access to those deemed illegal in that country or jurisdiction.
- iii. Telecom Service Providers (TSPs) are NOT the Internet. They invest in AND operate access networks to the Internet.
- iv. While the Internet has been around for many years and so have access providers, it is only in recent years that the Internet is becoming a commercially valuable

commercial marketplace – and consumers represent that value. This last point explains the motivations of some of those who oppose Net Neutrality.

- v. Further compounding the consumer's interest is the fact that in India, competition and choice are very limited. Fixed broadband options are very few. There are serious shortcomings in consumers' ability to choose, as the dismal service standards amongst some TSPs prove. With the proliferation of tablets and smartphones, mobile Internet providers are increasingly the go-to access providers. Mobile broadband and Mobile Internet are the fastest growing segments amongst access providers. Here too the market is dominated by two or three players. Portability and choice is dis-incentivized because data is an add-on to telephony services and that further limits the choice and ability of consumers to move. Compounding it all further is the fact that the sector has a long standing track record of poor Quality of Service(QoS), and the Regulator/Government - a poor track record of regulating for consumers interests.
- vi. It is in this uncompetitive landscape that TSPs, i.e. access providers with significant market presence/power and are outside the Internet are attempting to create exclusive platforms that are akin to preferred islands on the Internet, are offering services and applications.
- vii. The main focus of the Net Neutrality debate in India, is whether these access providers should be permitted to create these preferred islands over the Internet, and also regulate access through pricing and Quality of Service to the rest of the Internet. Creating a situation that the access networks would become Gatekeepers to the Internet, whilst "moving up the stack". This simple issue lies at the heart of the Net Neutrality debate.

B. FORMAL QUESTION WISE RESPONSE TO CONSULTATION QUESTIONS:

Question 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?

At the very outset, there is a need to define Net Neutrality. It is due to the absence of a definition on Net Neutrality, that a variety of stakeholders with distinctly different interests, are today claiming to be *for* it, thereby creating considerable ambiguity in the thriving national discourse on the issue.

The TRAI must in its definition of Net Neutrality, clearly delineate the basic principles of Net Neutrality, aka 'red lines' to protect the Consumers right to a free, fair and open nature of the Internet. As I have stated in my formal submission to the TRAI Consultation Paper on '*Regulatory Framework for OTT Services*' dated 23rd April 2015, the defining values of the Internet are its neutrality to content and participants.

While TSPs are legitimately entitled to maximize their business interests, they must do so fairly, without prejudicing the rights of the Internet consumers or by altering the free and open character of the Internet. All forms of Gatekeeping or 'Cabelization' by TSPs are a clear and present danger to the growth of the internet must be explicitly prohibited.

More significantly, TRAI must address Net Neutrality in a holistic manner, and do away with the piecemeal manner in which it has addressed the issue so far. While formulating its regulation, TRAI must consider the following aspects/issues, keeping in mind the uniqueness of the Indian context:

- i. Overall public policy, considerations and priorities;
- ii. Consumer interest, including issues related to access;
- iii. Commercial issues;
- iv. Technical issues;
- v. Legal issues impacting the rights of various stakeholders;
- vi. Security issues – impacting national security and network security;
- vii. Privacy and related issues.

The core principles of Net Neutrality should be as follows:

- i. Prohibiting TSPs from *blocking* applications, websites or other content on the Internet;
- ii. Prohibiting TSPs from '*throttling*' or slowing down Internet speeds;
- iii. Prohibiting TSPs from treating access to some applications, websites or other content on the Internet *preferentially*;
- iv. Prohibiting TSPs from imposing *differential tariffs* for data services based on applications, websites or other content on the Internet, without a prior examination and clearance by the Competition Commission of India and the TRAI;
- v. Prohibiting TSPs from using *Deep Pack Inspection* technology to inspect the contents of data packets.
- vi. Clearly and Unambiguously defining what constitutes "reasonable traffic management" practices post an extensive multistakeholder consultation.
- vii. Ensuring that TSPs make available in the public domain, detailed information about their activities such as their traffic management principles, bandwidth and pricing. The purpose of providing this information is to make sure that internet users can make an informed choice while choosing an TSP for themselves.

I am expanding on issues of Blocking, Throttling and Differential Pricing as described by Professor Vishal Misra, Columbia University:

1. Blocking by TSPs not permissible - All sites and apps must be equally accessible: TSPs and telecom operators should not block certain apps and sites, just because they don't pay them a revenue share. No gateways to the Internet should be allowed, and no preferential listing of certain sites, whether via commercial arrangements or not.
2. Throttling by TSPs not permissible - All sites must be accessible at the same speed (at a TSP level): This means no speeding up of certain sites because of business deals. More importantly, it means no slowing down some sites.
3. Differential pricing by TSPs not permissible - The cost of access must be the same for all sites (per Kb/Mb or as per data plan): This means no "Zero Rating", or differential rating for different sites, apps or services. In countries like India, Net Neutrality is more about cost of Internet access than speed of Internet access, because we don't have fast and slow lanes: all lanes are slow.

Question 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?

While Traffic Management is a necessity for TSPs to ensure smooth operation of access to the Internet, use of this power has to be clearly regulated and prescribed to ensure Net neutrality. Misuse of this explicit power will lead to violations of Net Neutrality.

TSPs can use a range of techniques for Traffic Management, including slow-down/speed-up (slow lanes/Fast lanes) of data to and from sites, preferential treatment to certain sites, (for example, sites that belong to the TSP or sites that have paid the TSP for this purpose), throttling internet access speeds to certain sites, and certain types of discrimination.

It is clear that such practices such as ‘Paid Prioritization’ of content or ‘Throttling’ of Internet access run contrary to the core principles of Net Neutrality, and must therefore be restricted. The US Regulator FCC, in February 2015, clearly stated that:

‘...Broadband providers may not favor some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind—in other words, no "fast lanes." This rule also bans TSPs from prioritizing content and services of their affiliates...’.

So, there is a need to regulate and prohibit traffic management by TSPs and carve out only a small exception to this prohibition.

These exceptions or what would constitute as ‘reasonable’ traffic management practices, (such as to deal with network congestion) requires a detailed examination from the stakeholders in the technical community. Stakeholders must engage in an exhaustive, nation-wide consultation on the issue. It must be acknowledged that the real solution to this problem is the overall improvement in network infrastructure, and therefore the

consultation must address the issue of network congestion and capacity on 2G and 3G mobile broadband networks.

Professor Vishal Misra of Columbia University has described some scenarios that can call for Traffic management exceptions:

- a) **Unforeseeable and temporary congestion:** When a wireless or land-line network goes through a period of unforeseen congestion (e.g. in the case of equipment failure), network operators are entitled to temporarily implement discriminatory traffic management practices in order to ensure to fluidity of data streams. But every time, operators must be able to prove to the regulatory authority that such congestion of its network was not foreseeable and that it took necessary steps to correct it. If the deployment of very high broadband networks takes longer than expected and operators face a durable saturation of their network, then the available bandwidth should be shared equally between all the subscribers and all service providers, until operators invest to upgrade their infrastructure.

- b) **Security threat on the network:** In case of an sudden attack or all other event undermining the proper operation of the network, discriminatory practices are also legitimate. But they should be circumscribed to temporary traffic hazards. Malicious actions aiming at altering the global operation of the network, whether intentional or accidental, should be considered as attacks. Traffic hazards needs to be addressed through temporary measures, either manually – when irregular traffic is detected – or automatically – when such traffic hazards are already well-known. The duration of these measures should not exceed that of the attack. They should be made transparent in order to foster collaboration among the community of network operators and allow for both a sound diagnosis of security threats and for the adoption of the most adequate methods to deal with them.

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

The consultation on Net Neutrality must ensure that TSPs are prevented from Cabelizing the net. For this, the TRAI regulations must be sound and enforceable.

Net Neutrality rules must be clear and unambiguous and Enforced - The policy and regulatory approach to Net Neutrality hinges around clear and unambiguous rules, including red line, no-go areas to be hardcoded into legislation and licensing agreements of TSPs. Further, the approach to Net neutrality must have clear Institutional responsibility in terms of Enforcement and punishment for violators.

Net Neutrality is a critical consumer Right, as is the role of the regulator in maintaining a free, fair and open nature of the Internet as part of its mandate of protecting consumer Interest.

Net Neutrality means no gatekeeping or Cabelization of Internet - To ensure Net Neutrality, is to ensure laws/regulation to prevent 'cabelization' of the Internet, i.e., no gatekeeping by TSPs.

There is substantive evidence in India of the market power of cable operators, and of the misuse, pricing abuse and distortions that helpless consumers have to suffer when access providers start controlling and influencing access to content. This Gatekeeping power of the access providers is unique because of the finite number of access providers in competition, and creates permanent distortions which even regulation can't manage today. This, in turn, creates a situation where rampant price gouging and/or poor quality is inflicted upon consumers, leaving them hapless except for upgrading to more expensive options. Cabelization of the Internet causes vertical integration which would lead to TSPs owning parts of the net and impacting consumer choice and competition in the long term by making web-only entities unviable and unable to compete. There is

ample evidence of that in the Indian Television and Media sector where vertically integrated entities have distorted choice and innovation, and have created market power concentration.

Policy action to start with Government - But it is to be noted that given the weaknesses in TRAI's powers in enforcing consumer rights and a weak track record of both the DoT and TRAI in protecting consumers' interests, much of the policy and regulatory approach will start with clear, decisive policy action on part of the DoT and Government. If required suitable amendments will need to be made to the TRAI Act and IT Act to ensure effective enforcement of Net Neutrality once finalized.

Prohibit Gatekeeping , Continuing Regulation for Free and Fair competition on the web - While the issue and risks from TSPs' gatekeeping are well understood and must be regulated against by clear prohibitions, the regulation of the web/Internet must be light and must not stifle creativity or innovation. The concept of continuing surveillance as a substitute to ex-ante bans must be preferred. The issue of distortions created by large Web entities is best regulated under Competition laws and regulation – because that is what it represents – distortions of competition on the Internet. This threat to free and fair competition also is a real threat to the open nature of the internet, but is best separated from Net neutrality and treated as what it is – Free and fair competition on the web.

As I have said earlier – TRAI must explore and develop joint forms of regulations on this type of competition and distortions on the web (outside the issue of Access power and Gatekeeping of TSPs) . It is for the TRAI to evolve an effective, capable and transparent form of regulation, either jointly with other domain expert regulators like the Competition Commission of India or on its own. A collaborative regulatory approach with other regulators that must be explored and developed.

Question 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.

The National Security Interests will and must supersede Rights to privacy and Net Neutrality. This must cover all apps, TSPs etc that operate in Indian jurisdiction.

However this power in case of National Security must be properly and transparently legislated – defining Agencies with power to surveill and intercept, personnel within these agencies and their powers and responsibilities and conditions under which these powers can be exercised.

The use of Deep Packet Inspection - which otherwise would be a prohibition under Net Neutrality and Privacy laws – could be used by National Security Agencies to snoop and monitor Internet traffic. However it can be envisaged that these Agencies may have powers and rights to seek TSPs assistance in DPI of target packets/communication.

However it must be noted, that while it is acceptable to expect Consumers to forgo rights to privacy and Net Neutrality under these circumstances, these must be exceptional circumstances backed by law. There are cases of DPI being misused in India by TSPs, for e.g. in December 2014, when Airtel attempted to introduce separate packs for VoIP calls.

‘Deep Packet Inspection‘, has implications of filtration and privacy, as TSPs will then have the ability to tracking what consumers are using their mobile Internet connection for. Airtel and Uninor have mentioned such plans in 2014.

A second concern arises from the IT Act’s provisions pertaining to National Security – which are at present woefully inadequate and unclear – and therefore unable to regulate or enforce penalties on TSPs when they attempt to misuse DPI. The solution for this may

be to review and amend the IT Act and ensure that laws of India are FULLY enforceable if and when violated by apps, service providers, content providers and Intermediaries.

While keeping in mind the above concerns, it must be reiterated that the legitimate cybersecurity concerns of the Government must not be mixed up in a discussion of Net Neutrality. As I had stated in my formal submission to the TRAI Consultation on *“Regulatory Framework for Over The Top Services”* dated 30th April 2015, there should be no attempts to introduce regulation that dilutes Net Neutrality under the guise of ensuring Security. National Security, Cyber Security and Cyber-Crime should be and can be examined separately from the issue of Net Neutrality , because the principle of suspension of rights under circumstances of National Security can prevail.

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

Please refer the response to question 4 above.

The conflict between National Security and Privacy is not a new one, and is obviously more pronounced as threats to National Security move online. However, a robust Privacy architecture that balances both the Privacy of the large majority of law-abiding citizens as well as National Security requirements of the country in dealing with threats – perceived or real - has to be architected.

Currently, incursions of Privacy are tried under the IT Act, 2000. However, as I had pointed out in a letter to the Minister of Communication and Information Technology in September last year, there are some glaring gaps in the existing privacy in the current legal data privacy protection framework as envisaged under the IT Act. These include:

- i. Expansion of the definition of sensitive personal data under rule 3 of the Sensitive Personal Data Rules: The categories of sensitive personal information, as identified in rule 3 privacy rules (passwords, financial information, sexual orientation, etc) are too narrow, restrictive and inadequate. So, other categories of information like mobile big data, M2M data, user behaviour, etc, should also fall within the ambit of 'sensitive personal data'. Emails and chat logs as well as records of internet activity, including online search histories, are particularly vulnerable to abuse and misuse, and should be accorded privacy protection.
- ii. Data protection provisions to extend to government agencies, not-for-profits and others: Section 43A of the IT Act, which was quoted by the ministry in its response to my question as a "protective provision", only covers the narrowly-defined 'body corporates' engaged in 'commercial or professional activities'. Thus, government agencies and non-profit organisations are entirely excluded from the ambit of this

section. This is a big hole, given that the government is a significant if not the biggest custodian of data relating to citizens.

- iii. Flaws in the drafting of section 72A of the IT Act: Section 72A, another provision quoted in the ministry's response, is a problematically-worded provision—it requires that third parties or intermediaries can only be held liable if it is proven that they have made a violation “with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract.”

This is flawed and is a much too broad test of privacy. It has to be much narrower—as in used for purposes other than that for which data was collected or unauthorised collection of data. In early 2015, Airtel was exposed as collecting user browsing information unauthorised, as did MTNL—and as both cases showed us, this is exactly the defence that most errant parties have invoked in order to escape being pinned on violations of privacy.

- iv. Reissue affordable standards that are equivalent to ISO/IEC 27001: The current standard prescribed by rule 8(2) of the IT Rules is the IS/ISO/IEC 27001 on “Information Technology-Security Techniques-Information Security Management System-Requirements”. To achieve ISO/IEC 27001 compliance and certification, the implementing body must have access to the copy of the standard, which adds cost. The costs of implementing this prescribed standard are further inflated by the involved costs of literature and training, external assistance, technology, employees' time and certification. This makes it beyond the reach of small and medium-sized Indian body corporates. In order to ensure adequate implementation of this, the ministry should, along with the BIS, reissue affordable standards that are equivalent to ISO/IEC 27001.

It is clear therefore that the current legislations and statute book do not provide enough by way of rights of privacy to an Indian citizen. The Privacy Bill 2014 needs to be discussed in detail in Parliament, and a new framework that guarantees citizen's right to privacy needs to be enforced. But this is beyond the scope of this consultation and needs a wider debate in country and Parliament.

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

There is no need for any explicit policy framework to defining relationship between TSPs and OTT content providers that needs Government or regulatory intervention. This demand is being made only by TSPs with no reciprocal call from the countless content providers out there.

It is surprising that the TRAI poses this question which makes an inherent assumption on the need for regulating the relationship between TSPs and OTTs. The TRAI overlooks its own observations in a December 2006 Consultation Paper titled “Regulating Internet Services.” Page 27 of the paper defined Net Neutrality as *“the principle that Internet users should be able to access all content they view and all applications they use on the Internet without being discriminated by Internet service provider(s)/ access provider(s).”* In fact, the 2006 paper had also cautioned against a future possibility of a violation of Net Neutrality principles, by stating *“The situation may also rise in India as Internet access providers may use their market power to discriminate against competing applications and/or contents.”*

There is no similarity between services provided by TSPs i.e. providing access to the Internet, and services ON the internet i.e. applications and content that use these access pipes to provide innovative technological services.

The Consumers Right to for a free, open and fair internet, however must supersede the TSPs’ objectives of maximizing commercial value by misusing control of access to the internet. Internet based innovations are disruptive to the internet landscape, but bring a host of transformative benefits to citizens and the economy. These cannot and must not be denied to consumers because of TSPs who are interested in maintaining the status quo.