
# Submissions to the Telecom Regulatory Authority of India on the Pre-Consultation Paper on Net Neutrality dated 30th May 2016

The Centre for Law & Policy Research ("CLPR") is a non-partisan, not-for profit law and policy research institution based in Bangalore. CLPR has been active in the field of media law and telecommunications regulation and offers wide ranging expertise in such fields.

At the outset, we support the core principles of net neutrality: non-discriminatory treatment of both content and applications using the Internet. Network neutrality is best defined as a network design principle that requires a public information network to treat all content, sites, and platforms equally and carry every form of information and support every kind of application.[1] The other major principle that motivates our responses is the principle of administrative forbearance which requires regulatory agencies to have a hands off approach to the relatively nascent field of Internet regulation and act only when there is a failure of other applicable private, public and criminal law to maintain net neutrality. Rapidly changing technology and user requirements have made it very difficult for conventional forms of regulation to be useful or comprehensive.[2]

**Our reply to the key questions:**

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?**

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

[2] 125 YALE L.J. 1548 (2016)

As mentioned earlier, the core principle of net neutrality is the equal treatment of all data and applications by the TSP. This must be understood in terms of the speed by which the data is transmitted and the cost to access such data or applications.

The primary goal of net neutrality are:

1. A competitive market place that generates the greatest economic value for the society.
2. Allowing for unfettered communication platforms that allow consumers and citizens to associate and express themselves freely.
3. A technology platform that encourages and sustains radical innovation and maintains an even playing field between incumbents and new market entrants.

This is particularly necessary in the current Indian context. The mobile revolution in India and the rise of numerous Internet based apps indigenous to India has been particularly visible. Anti-competitive practices through abrogation of these principles are known to directly stifle the growth of entrepreneurship that the government is attempting to foster.[3] In this regard it is useful to conceptualise Telecom Service Providers (TSPs) as gatekeepers whose only function is to provide access to the user to the Internet. This does not give the power to the TSP to decide what the user may choose to do once he/she has accessed the Internet.

**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?**

The goals of reasonable traffic management processes and the goals of net neutrality are arguably aligned.[4] He notes that certain forms of applications and content on the internet need a certain quality of service (QoS) in order to be usable. Examples of this include video streaming services which need a certain minimum bandwidth to be usable. Seen in this light, maintaining a minimum QoS benefits both consumers and content providers.

---

[3] This view has been taken by nearly 700 start-ups in India. See generally "Nearly 700 startup founders urge PM Modi to defend net neutrality", the Times of India, 26th January 2016, available at http://timesofindia.indiatimes.com/tech/tech-news/Nearly-700-startup-founders-urge-PM-Modi-to-defend-net-neutrality/articleshow/50729785.cms

[4] Tim Wu, *Network Neutrality, Broadband Discrimination,* Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003 at p. 155

However, it must be noted that the burden of maintaining a minimum QoS is primarily on the TSP. The TSP is bound by its contract with the user to provide a certain minimum QoS. The mere fact that the TSP may have too many subscribers does not release the TSP from its contractual obligations.

In this light it is necessary to establish that the first and foremost responsibility for maintenance of QoS is on the TSP and consider efforts made by other jurisdictions:

The US Open Internet Order 2010 says that

*"Legitimate network ensuring network security and integrity, including by addressing traffic that is harmful to the network; addressing traffic that is unwanted by end users (including by premise operators), such as by providing services or capabilities consistent with an end user's choice regarding parental controls or security capabilities; and/or reducing or mitigating the effects of congestion on the network."* [5]

In the EU, the following traffic management measures may be employed:

*"Reasonable traffic management measures shall be transparent, non-discriminatory proportionate and necessary to implement to :*

a) *implement a legislative provision or a court order, or prevent or impede serious crimes;*
b) *preserve the integrity and security of the network, services provided via this network , and the end-user's terminals;*
c) *prevent the communication of unsolicited communications to end-users who have given their prior consent to such restrictive measures;*
d) *minimize the effects of temporary or exceptional network congestion provided that equivalent types of traffic are treated equally.*
e) *Reasonable traffic management shall only entail processing of data that is necessary and proportionate to achieve the purposes set out in this paragraph."* [6]

The case of Japan in this context is particularly useful. As noted in the pre-consultation paper, Japan (along with South Korea) offers the fastest commercially available internet speeds in the world and therefore represents the gold standard for best practices in tackling network congestion.

---

[5] Available at https://apps.fcc.gov/edocs_public/attachmatch/DA-12-740A1.txt.
[6] Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013AR5960

It may be noted that the approach of the EU and the USA does not ensure the upgrading of the infrastructure of TSPs. The directives of the EU are further weakened by the fact that the TSPs are given the discretion to act proportionally which gives TSPs immense power to slow down or block content on a discretionary basis. On the other hand, the Japanese principles mentioned above do not have such legislative loopholes and are therefore a more complete code.

In light of all of this, the following principles may be employed in India:

1. The first response for a TSP should be to improve the infrastructure in place. It has been noted in the pre-consultation paper that the improvement of infrastructure in India is an absolute necessity. TSPs should not be allowed to disassociate themselves from their own responsibility in case of network congestion.
2. TSPs may only act against specific heavy users in the exceptional circumstances when their actions are affecting the overall quality of the network and thereby affecting the average user of the network.
3. There must be informed consent on the part of consumers. All consumers must be informed of all forms of traffic shaping that may be employed by TSPs.
4. Deep packet inspection as a form of traffic management may only be done where there is a need to protect the security and integrity of the network.

The decisions which users make are often determined by the Quality of Service that they get. As a result, TSPs should not know which applications are using its network as allowing for this knowledge may allow TSPs to favour certain content over other content in the name of network congestion.[7] The consumer should be given the autonomy to decide whether and when to use which service.[8]

If QoS is made chargeable then the network provider has an incentive to degrade the quality of the baseline, best-effort service to motivate users to pay in order to avail of an enhanced type of service.[9] The regulatory authority should set minimum quality standards so as to ensure that the quality of the baseline service fall does not fall below appropriate levels.[10] This user-controlled

[7] Ibid, p.135
[8] Ibid
[9] Ibid, p. 134
[10] Ibid, p. 135

Quality of Service offers an amicable solution to the problem of traffic congestion[11]; and preserves the principles of user choice and the principle of innovation.[12]

This is further subject to certain reasonable exceptions that may be caused due to technical faults in the network. These exceptions have best been summarised by NASSCOM in their response to a previous TRAI consultation paper:

1. Congestion caused due to temporary equipment failure. This is subject to the stipulation that such slowdowns are unforeseeable and that the TSP corrected the issue as soon as possible.
2. Slowdowns caused by attacks made to the network using malicious software.
3. The prioritisation of emergency services which may be declared to be in public interest by TRAI or another governmental agency.[13]

These principles may be misused in the following ways:

1. TSPs may attempt deep packet inspection where it is not necessary. The utmost stringency would have to be maintained to avoid such practices. Any unnecessary attempts at deep packet inspection must be treated as violations of customer privacy.
2. TSPs may make no attempt at improving infrastructure despite a rapidly growing consumer base. TSPs must be held accountable for providing the QoS promised to users in the Terms of Service.
3. TSPs may attempt to perform deep packet inspection of heavy users of a network. Such practices are directly contradictory to net neutrality as they discriminate based on the content of network usage.
4. The information provided by TSPs to the costumer regarding traffic shaping may be incomplete or incorrect.

In conclusion it is seen that the primary burden of ensuring a QoS must be on the TSPs themselves. The exceptions to be made to the aforesaid principles are only in case the network is being attacked by a user, if there are unexpected outages in the network or if the network is needed for emergency responses. Any network management made for any of these reasons must

---

[11] Ibid
[12] Ibid
[13] NASSCOM, *Response to TRAI Consultation Paper on Regulatory Framework for OTT Players*, http://trai.gov.in/comments/23-April/Attachments-23/NASSCOM%20Response%20%20to%20TRAI%20Consultation%20on%20OTT_Apr%202015.pdf.

be done in a content neutral manner. Such network management practices must also be made clear to consumers beforehand.

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

TRAI must adopt a stand of forbearance wherein the approach should be to intervene only when basic principles of net neutrality as mentioned earlier are threatened when the private parties fail to comply with net neutrality. In light of this, TRAI must not come up with hard and fast regulations to protect principles of net neutrality. Nations like the U.S.A, have been adopting the forbearance approach for most issues relating to net neutrality.[14]

As stated earlier, net neutrality is best understood in terms of competition law and the need to prevent anti-competitive strategies. If TSPs are allowed to serve as a gatekeeper for content rather than as merely a service that grants access to the Internet, it allows for numerous anti-competitive agreements between TSPs and content providers. This in turn has a knock on effect on entrepreneurship and small Internet based businesses.

However, it must be noted that other issues related to TSPs and access to the internet are already governed by other laws, such as consumer protection laws, contract laws and even criminal laws. These areas do not need further regulation by TRAI.

Consequently, India must have a strong, definitive and comprehensive policy on net neutrality but recognise that regulation must be strictly limited to the maintenance of the core principles of net neutrality.

**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 pre-consultation paper deems VoIP services a threat to national security due to a lack of oversight. However, no specific analysis has been made as to how VoIP services are a threat to

[14] What the Net Neutrality Rules Say, New York Times, March 12, 2015

national security. For the purposes of this response, it is assumed that such services may be used by terrorism organisations or similar anti-national elements thus threatening national security.

**The Indian framework adequately regulates VoIP calls:**

Currently, the framework for wiretapping telecommunication services is provided for under Sections 5(2) of the Telegraph Act, 1885 and Section 419A of the Telegraph Rules, 1951. These provisions specify a detailed procedure by which an investigating authority can legally wiretap a phone.

It may be noted that Section 3 of the Telegraph Act defines telegraph as follows:
*'telegraph' means any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means.*

*Explanation:—'Radio waves' or 'Hertzian waves' means electro- magnetic waves of frequencies lower than 3,000 giga-cycles per second propagated in space without artificial guide*
In light of this definition, VoIP services and internet messaging services are included under this definition. Rule 419A of the Act[15] would equally apply to VoIP services and internet messaging.

More importantly, Section 69 of the Information Technology Act, 2000[16] specifically provides for the decryption and of internet messages and calls in the interest of national security. The

---

[15] The Section *inter alia* provides that Directions for interception of any message or class of messages under the Indian Telegraph Act, 1885 shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government. In unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorized by the Union Home Secretary or the State Home Secretary, as the case may be:
Provided that in emergent cases—
(i) in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or
(ii) for operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible.

[16] 69 Power to issue directions for interception or monitoring or decryption of any information through any computer resource. -
(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.
(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

Section further provides for a punishment of 7 years imprisonment in case any authority in this process fails to comply thereby ensuring prompt compliance.

The Justice A.P Shah Committee Report[17] has stated that the two legislations, the Telegraph Act and the Information Technology Act which govern law relating to interception must be amended as follows:

"*1) Consent and Choice: Individuals may not be given the choice of being monitored, and consent from the individual may not be required for an interception to take place.*

*2) Access and Correction: Individuals may not be able to access interception records pertaining to them during an investigation.*

*3) Notice: Authorized agencies may be required to provide notice of legal access after an investigation is closed."*

We endorse the aforesaid view taken by the Commission.

**International perspective:**

The use of private data by intelligence agencies in the name of national security must now be seen in the light of the revelations of Edward Snowden. Snowden's release of thousands of documents showing the true extent of snooping carried out by the world's most powerful nation has exposed the extent to which privacy has been compromised in the name of security.[18]

The US government has the power to wiretap VoIP calls under the Communications Assistance for Law Enforcement Act (CALEA). Enacted on October 25, 1994, CALEA requires a "telecommunications carrier," to grant access to equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," to law enforcement

---

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-
(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
(b) intercept, monitor, or decrypt the information, as the case may be; or
(c) provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

[17] Report of the Group of Experts on Privacy,Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court), available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

18 *Edward Snowden: Leaks that exposed US spy programme*, available at http://www.bbc.com/news/world-us-canada-23123964

once a court order has been received.[19] These provisions bear a significant similarity to Rule 419A of the Telegraph Rules. In light of Snowden's revelations, it may be necessary to review the mechanism of wiretapping not from the perspective of national security but rather the perspective of overreach by law enforcement agencies.

It may be noted that the blocking of VoIP services on the ground of national security is quickly becoming the hallmark of authoritarian governments as evidenced by the policies in China, Libya, Egypt, Iran, Morocco, North Korea, Syria and Turkey. However, the aim of the relevant governments there has been to prevent political dissent and ensure their continuity in power.[20]

In light of all of this, it must be noted that since India already has an extremely comprehensive framework in place for the wiretapping of VoIP calls and decryption of Internet messages. Instead, further regulation may be deemed necessary to prevent the overreach of law enforcement agencies in this regard.

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

The pre-consultation paper suggests that VoIP services may compromise the privacy of a consumer. The paper does not provide for reasons as to how this would come about. Moreover, there is no apparent reason that VoIP services would be more vulnerable to questions of privacy as compared to other forms of communication over the Internet. Activities such as phishing[21] are rampant and are a much greater threat to consumer privacy than the disclosure of personal information through VoIP services.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), Rules, 2011 requires every service provider to outline a detailed privacy policy that is applicable to all users, that articulates the nature of the data collected, type

---

[19] Communications Assistance for Law Enforcement Act, available at https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

[20] Sulayman Makalo, *Blocking the VoIP services for national security reasons is illogical*, available at https://americanstreetnews.com/blocking-the-voip-services-for-national-security-reasons-is-illogical-says-sam-phatey/.

[21] The term phishing has been defined by the Merriam-Webster dictionary as:
*a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly*

of data that is collected and for what purpose including retention and further use.[22] This would cover any data being collected by any VoIP service providers and internet message clients.

Further, it may be noted that VoIP calls are not susceptible to attacks from hackers or those seeking to access private information as no record of the content of the call remains after the call is completed. In fact, there is no way for a Telecom Service Provider (TSP) or a government regulator such as TRAI to recognise that data packets being sent over the internet contain VoIP messages without a deep packet inspection. Such an inspection (and any subsequent discrimination based on the inspection) would amount to a fundamental violation of the policy against data discrimination which is one of the core tenets of net neutrality.

Finally, this proposition is at odds with the argument that VoIP calls threaten national security. The assertion that VoIP services compromise user privacy suggests that the calls so made are not secure. However, the argument that VoIP services compromise national security is based on the presumption that such calls are impossible to access or tap. There is therefore a fundamental contradiction between the two arguments raised.

In conclusion, it must be noted that any private data collected by any OTT service will be subject to The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), Rules, 2011. In addition, VoIP calls in particular are far less likely to lead to the leaking of private consumer data as such data is usually not recorded by the OTT provider.

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

Further issues to be considered are as follows:

VoIP services and telecom services exist on an uneven playing field:

[22] Available at http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf .

The pre-consultation paper suggests that since VoIP and telecom services perform a similar function, they should be regulated similarly. However, this argument has notable flaws.

While VoIP and telecom services perform largely the same function, they are performed through different media. They are not directly competing services as a result and the argument that there is no level playing field between them is not applicable. This may be explained using an example. E-mail and regular post perform largely the same function. However, it cannot be expected that the two have similar pricing structures. While it is true that e-mail has vastly reduced reliance on regular postage, it cannot be said that regulators must slow email to the speed of regular post and introduce a similar pricing structure in order for regular post to compete with e-mail. It is generally understood that the two are entirely separate services.

Further, the difference between the pricing of VoIP services and regular telecom is not a result of the regulatory framework in place for telecommunication services. Instead, the difference arises as a result of the vastly different infrastructural and technical means by which messages are sent in these two forms of communication.[23] VoIP delivers voice transmissions over a broadband internet connection instead of using the platform provided under a public switched telephone network, which happens to be the mode for enabling functioning of traditional telephones.

Therefore the foundational assertion that VoIP services and regular telecom services should be regulated equally with a similar price structure is not appropriate and should be reconsidered.

Zero-rating

Another issue regarding the relationship between OTT providers and TSPs is the practice of zero-rating or toll free data. Zero rating refers to the practice by which a TSP provides free data which can only be used for a particular application data. Through zero rating, large providers would be able to treat both applications and content in a discriminatory manner. If they are permitted to do so, the access to content and applications would be conditional upon a lucrative deal with the network providers.[24]

---

[23] Rekha Jain, Radha Ravattu, Rishabh Dara, Response to TRAI Consultation Paper on Regulatory Framework for Over-the-top (OTT) Services, 27th March 2015, available at http://cis-india.org/internet-governance/resources/net-neutrality/2015-03-27_cis_trai-submission_regulation-OTTs.

[24] Michael Geist, *'Zero rating' battle throws net neutrality in doubt: Geist,* Toronto Star, July 4, 2016

In light of the TRAI consultation paper specifically on this subject[25], we will not go too deeply into this question here. However, it must be noted that such policies are also inherently anti-competitive and in violation of the principle of net neutrality.

Fast lanes:

'Fast lanes' refers to the practice where TSPs can charge specific OTTs like YouTube and Netflix so that content is available to the consumers at a higher speed, for these content providers.[26] The concept of fast lanes is anti-competitive because only those OTTs who can pay for the fast lane to the provider would be able to provide content to the users at a high speed.[27] This practice is in violation of the principles of net neutrality.

Free Basics

Under Free Basics a particular content service provider (or providers) provides its own content free to consumers, whereas the rest of the data has to be paid for.[28] This is again in violation of the principle of net neutrality. The Federal Communications Commission, through its Open Internet Order released March 12, 2015 has banned fast lanes or paid prioritization.[29] This was done to protect the open Internet[30] and the save consumers from confusion.[31] India must be vigilant about any attempts to set up similar fast lanes.

**Conclusion:**

The Centre for Law and Policy Research is happy to present its views for this consultation paper and are further open to present further arguments and analysis on this issue at TRAI's convenience.

---

[25] Consultation Paper No. 7/2016

[26] Hassan Habibi Gharakheili, Arun Vishwanath & Vijay Sivaraman, *Perspectives on Net Neutrality and Internet Fast-Lanes*, 46 Computer Communication Review 64, 66 (2016)

[27] ibid

[28] Parminder Jeet Singh, *Free Basics, now through the backdoor*, The Hindu, July 5, 2016

[29] Federal Communications Commission, The Open Internet Rules, GN Docket No. 14-28, FCC 15-24, Adopted: February 26, 2015, 5607

[30] Ibid

[31] Ibid at 5608.