SFLC.IN'S COMMENTS

CONSULTATION PAPER ON NET NEUTRALITY

Introduction

Before we address the questions in detail, we would urge the regulator to think about the current economy of the net. The Internet has turned into a behavior collection system and its made of things that are called telecommunications network. For Telecom Service Providers (TSPs), it now makes sense to carry people's packets for them in order to conduct social behavior collection – to perfect the social graphs and to engage in advertising, profiling of people. There is a whole range of activities that are possible that justify the cost of paying for people's telecommunications and so we are engaged in a great international conversation about the extent to which people's behavior should be collected on the basis of payments for their telecommunications services. Moreover, there have been troubling developments globally that make it ever easier for TSPs to engage in this social behavior collection. The recent repeal[1] of the United States Federal Communications Commission's broadband privacy rules[2], which would have banned Internet providers from collecting, storing, sharing and selling certain types of customer information without user consent, serves as an example.

World over, those who control the network engage with regulators such as TRAI within the context of concepts like Network Neutrality that don't have behavior collection as as an essential ingredient. For statutory reasons or otherwise, these conversations seem out of the jurisdictional or domain expertise bounds for telecom regulators, but it creates a blind-spot. Such a blind spot ignores that the Internet, which is the highway for new economy, is being converted into a one-way traffic medium, where with vertical integration of various businesses, content is being used as bait to bring people to a network that collects behavior. Your next consultation should contain a series of questions about TSPs becoming the new frontiers of behavior collection, ask about their processes

1 Brian Fung, *Trump has signed repeal of the FCC privacy rules. Here's what happens next*, The Washington Post, April 4, 2017, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/?utm_term=.6d2f5977251a

2 See the FCC Report and Order dated November 2, 2016, available at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1_Rcd.pdf

and how that fits into the larger question of creating prosumers. Sound policy making can no longer approach these intertwined issues severally or independently because increasing access must mean creation of empowered prosumers.

Responses to the issues for consultation

Q.1: What could be the principles for ensuring nondiscriminatory access to content on the Internet, in the Indian context?

In the Indian context, we recommend that a neutral and non-discriminatory Internet be guided by the following principles:

1. *No Application Based Discrimination:* TSPs should not discriminate Internet traffic based on content, any applications or classes of applications or services
2. *No Paid Prioritization:* TSPs should not be allowed to favor some content or traffic over another for any consideration, no "fast lanes" should be allowed.
3. *No Throttling or blocking:* All content should be treated equally and TSPs should not intentionally slow down the speed of some content or speed up others based on the type or TSP's preference.
4. *Transparency in traffic management:* The traffic management principles adopted by the TSPs should be transparent and application-agnostic and should primarily be used to achieve a legitimate traffic management purpose and not a discriminatory commercial purpose. Any traffic management practice adopted to comply with legal requirements or restrictions imposed by law enforcement agencies or the government must be subject to review by a committee.
5. *No Deep Packet Inspection:* No DPI should be allowed unless for specified reasons mandated by law and that should be made transparent.

Any rules that are adopted must ensure that user choice is preserved, and that TSPs do not discriminate on the basis of kind of applications, do not restrict freedom of speech and expression,

keep the entry barriers low and promote innovation. Moreover, the regulator should prohibit application-specific discrimination, but allow application-agnostic discrimination i.e. one that does not discriminate amongst applications or classes of applications. The Internet's original architecture was based on the layering principle and on the broad version of the end-to-end arguments.[3] As a consequence of that design, the Internet was application-blind – it was unable to distinguish among the applications on the network – and, as a result, it was unable to make distinctions among data packets based on this information. The Internet's application-blindness is one of the factors that have fostered innovation in the past and made the Internet more valuable for users and for society. Any NN framework must therefore be mindful of the Internet's application-blindness, and ensure that the only permitted form of discrimination is application-agnostic.

Q.2: How should "Internet traffic" and providers of "Internet services" be understood in the NN context?

(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.

Internet Services should be understood to include all services that use the Network of Networks, commonly known as the Internet. As a rule, all Internet services, should follow the core principles of Net Neutrality, as explained in the DOT Committee Report on Net Neutrality. The objective or the function of the Internet service may be a criterion to provide exemption from the Net Neutrality principles only in limited cases like Emergency services. Such services which can be exempted should be decided by the Regulator or the Government and should not be left to the discretion of the

3 David D. Clark, The Design Philosophy of DARPA Internet Protocols, COMPUTER COMM.REV., Aug 1988, p. 106

providers.

(a) Specialized services could affect other services of subscribers and hence should not be given any exemption from the core Net neutrality Principles. In the findings from BEREC's and the European Commission's joint investigation[4] it was found that "*About one third of the fixed operators indicate in their responses that specialized services are affecting, to some extent, the Internet best-effort service of customers using the same access network*". Thus, there should not be any exemption for specialized services or Internet of Things. Such exemptions could leave loopholes for the operators to push their services and business-models which could affect the interest of users accessing the "best-effort" Internet.

(b) With the emergent media technologies, we are already seeing a merger of traditional business models with the new ones, especially in the delivery of video content. CDN are being deployed for robustness of delivery and better end user experience. This has caused a sharp increase in the number of CDN Providers and deployment of own CDN by ISPs. With the increase in availability and demand of bandwidth intensive video content, traditional arrangements of transiting or peering will not hold and disputes about compensation are bound to occur. Various disputes between Comcast and Netflix in the United States are available as evidence.

In order to have more competition at the last kilometer and ensure creation of more services that may be bandwidth intensive, the regulator must ensure that , "toll-charges" are not extracted by ISP from the content provider and the CDN provider in addition to the payments made by consumers that subscribe to the ISPs services.

The regulator must also ensure that CDNs deployed by ISPs cannot just be restricted to the delivery of content to support the ISP's own 'walled garden' services or be subject to arbitrary demands of compensation. The regulator must endeavor to control the effort on part of the ISPs to provide, 'better than best efforts" , creating fast and slow lanes on

4 A view of traffic management and other practices resulting in restrictions to the open Internet in Europe is available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2039

payment of higher fee while intentionally degrading the standard service.

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

(a) Defining what constitutes reasonable TMPs (the broad approach), or

(b) Identifying a negative list of non-reasonable TMPs (the narrow approach)

We believe the broad regulatory approach to TMPs would be ideal in the Indian context. A narrow approach that identifies and prohibits a list of non-reasonable TMPs would not be sustainable in the long run, as such a list is likely to be made obsolete relatively quickly. Considering the pace of technological progress, it would only be a matter of time before fresh non-reasonable TMPs come to be deployed in place of the prohibited ones. Also considering the practical challenges involved in identifying and listing all non-reasonable TMPs in exhaustive detail, we recommend adopting a broad regulatory approach to TMPs, under which reasonable traffic management is recognized as an exception to the principle of NN, and the scope of reasonable TMPs is outlined in sufficient detail.

Q.4: If a broad regulatory approach, as suggested in Q2, is to be followed:

(a) What should be regarded as reasonable TMPs?

(b) Whether and how should different categories of traffic be objectively defined from a technical point of view for this purpose?

(c) Should application-specific discrimination within a category of traffic be viewed more strictly than discrimination between categories?

(d) How should preferential treatment of particular content, activated by a user's choice and without any arrangement between a TSP and content provider, be treated?

(a) TMPs can simplistically be termed as technical methods deployed by TSPs, by which Internet data packets are caused to be transmitted other than on a best-effort basis. As the

term suggests, the primary intent of TMPs is to manage congested networks – more specifically, to mitigate derogation of QoS on congested networks. TMPs are also deployed at times for such other reasons as ensuring smooth flow of latency-sensitive data and ensuring network integrity.

The "technical methods" deployed for these purposes may refer to a number of things, including methods such as Diffserv (Differentiated Service Label), ECN (Explicit Congestion Notification), RED (Random Early Drops), flow-based routing, traffic smoothing/packet grooming etc., as well as more invasive methods such as DPI (Deep Packet Inspection) and TCP reset injections.[5] While the principle of NN demands that all Internet data be treated equally, reasonable traffic management is considered an exception to this rule as it is a necessary technical component of network management. However, due to the risk of exploitative uses of TMPs, it is also necessary to clearly outline the scope of reasonable TMPs.

When determining the reasonableness of any TMP, we recommend that the following be considered as key parameters:

- *Motive:* All TMPs must perform strictly technical functions that are designed to meet specific technical requirements, be it management of network congestion, accommodating latency-sensitive traffic, ensuring network integrity, or others. Compliance with legal requirements, and accommodation emergency services may also be treated as permissible grounds for TMPs. On the other hand, no TMP must be deployed on the basis of commercial considerations such as promoting the content/services of particular providers over others, or demoting particular content/services. If commercially motivated TMPs were to be permitted, this would result in anti-competitive behavior that causes content/services from smaller providers to be shunned in favor of those from bigger players with vast financial reserves.

5 Campaign for Democratic Media, *Initial Comments on Review of the Internet Traffic Management Practices of Internet Service Providers*, February 23, 2009, available at: http://www.globalmediapolicy.net/sites/default/files/Argument_-_CRTC-PN2008-19_-_FINAL_-_23Feb2009.pdf

- *Proportionality:* Any TMP considered for deployment must be proportionate to the motive it seeks to fulfill. TMPs that impact more classes of Internet traffic than necessary, in more regions than necessary, and unduly invasive TMPs such as DPI that also infringe upon the users' rights to privacy and freedom of speech must be considered non-permissible.

- *Duration:* All TMPs must be limited in time i.e. they must be deployed on temporary basis. As traffic management primarily serves a strictly technical function of easing network congestion, TMPs must be deployed for only as long as the network congestion lasts, and must not continue once the congestion eases and they are no longer needed. As other grounds for reasonable TMPs such as ensuring network integrity, complying with legal requirements, and accommodating emergency services, are all non-permanent in nature, TMPs deployed for these reasons must also not continue beyond the duration of the reasons themselves.

- *Transparency:* TMPs must be deployed in a transparent manner, with adequate disclosures as to the nature of TMP deployed, the reason for which it is deployed, kind of content/services affected, and duration for which it lasts. Transparency is vital in traffic management, as it allows stakeholders to stay abreast of the ways in which TMPs are being undertaken, monitor such practices for NN violations, and make informed choices on the basis of this information.

(b) For the purpose of implementing TMP regulations, it is necessary to outline various categories of Internet traffic based on the nature of content being carried. This will allow for the objective identification of high-bandwidth traffic that needs to be managed to prevent overburdening networks, and also provide a basis for accurate disclosures as to the kind of TMPs adopted. The following could be some of the broad classifications of Internet traffic: browsing; peer-to-peer; email; instant messaging; VoIP; music streaming; video streaming; music downloads; video downloads; gaming; software updates.

(c) Any discrimination practiced while employing TMP should be application agnostic and should not differentiate between various applications in a category of service. Between categories of service, transparent methods may be used to achieve traffic management when strictly necessary. Discriminating amongst applications within the same category is unjustifiable under any circumstance, but discriminating amongst broad categories of traffic for technical reasons may be permitted so long as the established mandates of applicable regulations are strictly observed. Discriminating amongst categories of applications when there is no demonstrable technical or legal reasons to do so should be treated at par with application-specific discrimination.

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

N/A

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

(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.

In context of a broad regulation on TMPs, where traffic management constitutes an exception to the principle of NN and the scope of reasonable TMPs is clearly outlined, the above i.e. emergency

situations and services, restrictions on unlawful content, maintaining security and integrity of networks, and services notified in public interest may be treated as grounds for reasonable TMPs. In emergency situations, such as in the aftermath of a natural disaster, where other communication channels may be unavailable, Internet-based communication platforms could act as an alternate means to co-ordinate rescue and relief operations. Under such circumstances, prompt and reliable delivery of content would assume paramount significance, and could mean the difference between life and death as far as victims are concerned. As regards blocking access to unlawful content, regulatory mandates applicable to TMPs may be exempted because selective blocking of content in such cases would be done in furtherance of express legal directives. As service providers are bound to ensure compliance with legal obligations, blocking of particular content must not become grounds for presuming violations of applicable TMP regulations. A similar reasoning may be imported into discriminatory treatment of content and services that are notified in public interest by the regulators, so long as such notifications follow objective and clearly defined criteria to identify content and services deserving of differential treatment.

Therefore, in the above cases, departures from the best-effort delivery of Internet data may be permitted rather than considered violations of NN.

Q.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?).

(a) Blocking may be defined as “the practice of actively preventing users from accessing particular content and/or services available on the Internet, which they would otherwise

have access to".

(b) Throttling may be defined as "the practice of intentionally degrading quality of service when accessing particular content and/or services available on the Internet".

(c) Preferential treatment may be defined as "the practice of transmitting particular content and/or services available on the Internet at a higher priority than others".

As regards tests, thresholds and technical tools available to detect the deployment of blocking, throttling and preferential treatment, we would like to draw the Authority's attention to Measurement Lab (M-Lab) – a joint initiative by New America's Open Technology Institute, Google Open Source Research, Princeton University's PlanetLab, and other supporting partners.[6] M-Lab is an open source Internet measurement effort that provides a suite of performance tests to help consumers develop an accurate picture of their Internet services. The data collected during tests is also collected and released to the public for use by policy makers, researchers and others who are interested in Internet issues. The performance tests hosted by M-Lab notably includes a Network Diagnostic Test that tests connection speed and provides a detailed diagnosis of problems limiting speed, Neubot which performs periodic tests to measure network performance and traffic throttling, OONI Probe which measures specific use cases of network interference, and Glasnost which tests for application-specific blocking or throttling.

Each test hosted by M-Lab is independently developed by researchers, and each researcher-developed test is allocated dedicated resources on the M-Lab platform to facilitate accurate measurements. Server-side tools are openly licensed and operated, allowing third parties to develop their own client-side measurement software.

Q.8: Which of the following models of transparency would be preferred in the Indian context:

(a) Disclosures provided directly by a TSP to its consumers;

(b) Disclosures to the regulator;

6 See https://www.measurementlab.net

(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?

We believe option (d) i.e. a combination of all stated models of transparency would be ideal in the Indian context. Whereas disclosures of pricing information and commercial terms, performance characteristics, TMPs, and specialized services to existing consumers and the regulator must be seen as a mandatory, essential component of the NN framework under all circumstances, we believe disclosures to the general public would also be valuable as this will enable potential consumers to make informed decisions as to their choice of TSP after weighing all available options in an exhaustive manner. As the end-users' expectations from Internet services will see wide variance from person to person depending on their individual use-cases, having easy access to all relevant information as mentioned above would prove greatly beneficial to the general public.

Disclosures to existing consumers and the general public must be made in formats prescribed by Information Disclosure Templates issued by the regulator, such as that included in Chapter V of this consultation paper. These should be prominently displayed at all points-of-sale as well as on the websites of all TSPs in an easily accessible manner. As the regulator would require a higher-standard of disclosure with granular detail on all practices adopted by the TSP, a more detailed format for disclosures to the regulator may be stipulated. In addition, we also recommend that the regulator publishes a layman-friendly guide to enable end-users without technical knowledge to easily grasp relevant details from the information disclosures made by TSPs. The UK's Office of Communications has published a layman's guide to traffic management[7], which could serve as a point-of-reference for such an effort.

Q.9: Please provide comments or suggestions on the Information Disclosure Template at Table

7 Ofcom, *A Guide to Internet Traffic Management*, September 2013, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0012/6042/traffic.pdf

5.1? Should this vary for each category of stakeholders identified above? Please provide reasons for any suggested changes.

With respect to the Information Disclosure Template, we would recommend that the section soliciting information on application specific traffic management be omitted, since all permissible TMPs must necessarily be application agnostic as discussed previously. Perpetual blocking and/or prioritization of particular services, content, applications, or products, other than in compliance with legal obligations, would constitute unreasonable TMPs that must be prohibited under relevant regulations. Solicitation of information on these counts would therefore be unnecessary, and may accordingly be removed. In addition, if fields under "Application specific traffic management" are removed, the head "Application agnostic traffic management" may be renamed to "General traffic management" so as to better distinguish it from "User triggered traffic management".

We would also recommend that under the head of "Application agnostic traffic management", or "General traffic management" as applicable, the field that currently reads "Specify type of traffic (e.g. audio streaming, video streaming, P2P downloads etc.)" be expanded to individually account for all categories of traffic outlined in response to Q.4(b) i.e. browsing, P2P, email, IM, VoIP, music streaming, video streaming, music downloads, video downloads, online gaming, and software updates. In other words, TSPs may be asked to specifically state whether any such traffic categories are actively managed during peak hours, and if yes, to what extent and in what manner. This will ensure that subscribers and the general public are provided a more detailed insight into the TMPs deployed by TSPs, and it will also impose an additional layer of accountability on TSPs on account of their unambiguous declarations as to the nature of TMPs deployed as against specific traffic categories.

Q.10: What would be the most effective legal/policy instrument for implementing a NN framework in India?

(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?

We submit that the ideal instrument for implementing a NN framework in India would be an exhaustive Regulation issued by TRAI in exercise of powers conferred under Sections 36 and 11 of the Telecom Regulatory Authority of India Act, 1997. In addition, the Authority may also recommend amending the service licenses granted by the Department of Telecommunications to TSPs, so as to incorporate the core principles of NN into said licenses. A legislation enacted by the Parliament is yet another option to implement a NN framework in India, but in light of the significant delays involved in enacting such a legislation and updating it to keep up with evolving technologies, we consider a Regulation by TRAI coupled with amendments to TSP licenses to be the ideal instrument in the Indian context. Moreover, TRAI has the added advantage of having engaged in an extensive public consultation process specifically on NN, and is therefore most well-placed to implement a NN framework that addresses all stakeholder concerns.

While we do have an existing regulation on discriminatory tariffs, the said regulation addresses only one of the several issues pertaining to the Paid Prioritization or preferential treatment while leaving a host of other issues such as blocking and throttling unaddressed. Moreover, under the power given to the authority under the TRAI Act, another regulation on discriminatory QoS can also be put in place. But none of them will provide for a single window solution to all the problems emanating out of the violations of the core NN principles. Advancement in technology or a detection of a new anti-NN practice shall result in amendment in not just one but a multitude of places. Therefore, the most appropriate approach to this problem would be to put in place an umbrella regulation on NN, with bright line rules on blocking, throttling or preferential treatment, covering all the aspects of NN, incorporating in it the existing regulations on discriminatory tariff, provisions relating to QoS standards and the transparency measures to be undertaken.

(a) The ultimate body responsible for monitoring and supervision should be TRAI. As NN

violations require a very close and robust monitoring mechanism, this function can be delegated to a specialized cell within TRAI, established specifically for this purpose. Such a body shall look closely into the NN violations, identify the tests and tools that need to be adopted to detect such violations and in case of detection of any such violation, take necessary actions to address the same.

(b) Taking appropriate action in the event of detection of any NN violation is the most pertinent step towards ensuring compliance to the NN regulations. Imposition of penalties is one of the most effective tools which facilitate efficient enforcement of the rules. It serves as a deterrent and a dissuasive action. Thus, the regulatory authority should be empowered to impose heavy penalty or fines on the ISPs in order to deter them from indulging in such violative practices. Moreover, in cases of severe and repeated violations, stringent measures such as suspension of the ISP license for a limited time period or final cancellation thereof can be undertaken.

(c) The ultimate aim of these regulations is to promote and protect consumer interests and to encourage competition among the service providers. Though we do not recommend laying down separate QoS regulations on this matter, if opted for by the authority, such regulations should provide for the minimum QoS standards to be met by the ISPs to implement NN frameworks. For the purposes of ensuring NN, it should include bright line rules to prevent blocking, throttling or preferential treatment. It should further provide for the reporting and publication procedures to ensure transparency and an effective enforcement mechanism.

Q.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:

(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).

One of the biggest challenges in monitoring for violations of a NN framework could be detecting anti-NN practices deployed without public knowledge. For instance, if a TSP and a content provider were to enter into a discreet commercial arrangement, according to which the latter's content is prioritized over competing content from others, it would be very difficult, and in some cases, impossible, for third-parties including regulators, competitors, and the general public to recognize the deployment of such an arrangement without express declarations from either the TSP or the content provider in question. Anti-NN practices like throttling and paid prioritization would be particularly susceptible to going undetected when compared to those like blocking of content, as any deteriorations or improvements in QoS may easily be attributed to routine network fluctuations rather than deliberate actions.

Whereas a robust framework of legally mandated information disclosures by TSPs and proactive review by the regulator of information sourced from users, third parties and the public domain would certainly disincentivize TSPs and affiliates from violating any applicable NN frameworks, we recommend that TRAI also conduct periodic audits of TMPs adopted by TSPs. TMPs that are actively deployed may be evaluated against disclosures made by TSPs to regulators, users, and other stakeholders, and those found to use undisclosed TMPs or disclosed TMPs in ways that exceed their stated scope may then be heavily penalized. Similar audits are already being conducted by the Authority with respect to QoS, where external agencies are contracted to audit TSPs for compliance with QoS mandates as laid out in various Regulations on the matter.[8] A comparable model of external audits may be adopted by TRAI with respect to NN.

Q.12: Can we consider adopting a collaborative mechanism, with representation from TSPs,

8 Financial Times, *BSNL to Rope in Independent Agency for QoS Audit*, January 26, 2004, available at: http://www.financialexpress.com/archive/bsnl-to-rope-in-independent-agency-for-qos-audit/98259/

content providers, consumer groups and other stakeholders, for managing the operational aspects of any NN framework?

(a) What should be its design and functions?

(b) What role should the Authority play in its functioning?

A collaborative approach for managing operational aspects of the net neutrality framework would be of immense benefit to its effective implementation. Inputs from various stakeholder groups such as Government, industry, civil society, academia, technical community, and end-users will not only provide a detailed insight into the operational aspects of the framework, but also help formulate effective solutions to any problems that may arise.

(a) The collaborative mechanism may be set up in the form of an NN Steering Group with multi-stakeholder participation. Representatives from the stakeholder communities mentioned above may be selected based on their merits and contributions in the field of law and technology. This Steering Group should be responsible for reviewing compliance with NN requirements, addressing technical difficulties in their implementation, facilitating exchange of information about reasonable TMPs, promoting innovation, and identifying current and emerging issues related to implementation of the NN framework. It should also be able to provide assistance to the authorities, suo moto or on request, on matters within its competence.

(b) The authority should only play an advisory role in its functioning. Its main function in the Steering Group should be to assimilate the information and recommendations so obtained and further process it towards effective policy implementation. The Steering Group should be able to provide a quick, non-Government driven platform which offers scope for open and meaningful discussions and solution-based approaches to the problems surrounding the NN framework.

Q.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?

On account of the rapid rate of technological progress, it is crucial that laws and policies governing the use of technology keep pace with the technologies they seek to regulate. Failure to do so may result in the imposition of undue restrictions that in turn may hamper innovation and limit growth in the industry.

Implementing applicable laws and policies in a manner that is amenable to relatively frequent updates is an important first step in ensuring sufficient regulatory flexibility. Enforcing the NN regulatory framework as a Regulation by the Authority rather than an Act of the Indian Parliament would help keep procedural hurdles to a minimum when it comes to amendments. As neither the initial enactment nor subsequent updates would need to follow Parliamentary procedure involving assent from Lok Sabha, Rajya Sabha, and the President, this would significantly reduce the amount of time required to translate regulatory changes from ideation to implementation, so that the very purpose of effecting said changes are not rendered moot by the time they are actually implemented.

The Authority may also rely on the multi-stakeholder community to be made aware of the need for regulatory reform. A NN Steering Group as discussed in response to Q.12 could play an integral role in collecting stakeholder feedback and conveying them to the Authority in a timely manner. The Steering Group would be well-placed to hold periodic meetings to go over current and emerging issues surrounding the NN framework, and it would also have the benefit of being informed by a direct multi-stakeholder consultation process. The Authority's own active involvement in such a Steering Group would further enhance its utility as a means to rapidly implement necessary regulatory changes when necessary.

In addition, the Authority may consider providing other platforms for public feedback on both conceptual and operational aspects of the NN framework. An open forum where the general public may submit their views on any aspect of the NN framework would allow the Authority to get a sense of the most common concerns and recommendations related to NN, which could then be used to initiate reviews of the NN framework based on a more detailed public consultation process such

as the present Consultation Paper. Periodic in-person meetings with representatives from each stakeholder group i.e. Government, industry, civil society, academia, and the technical community is yet another way in which the Authority could keep abreast of the need for regulatory reform.

Q.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

Device, browser, and Operating System (OS) deployed at the user-end can all impact the quality of Internet services. With user-end devices for instance, type of processor, hard disk, network and graphics cards, available RAM, all impact the speed at which the computer processes Internet data. Similarly, corrupted or poorly configured browsers may slow down Internet speeds, and multiple add-ons to the browser can also negatively affect Internet speeds. Corrupted and outdated OS, and the presence of multiple applications running on the device without the user's notice are yet other factors that tend to slow down Internet speeds. However, these aspects are unconnected to Net neutrality as these affect only the performance on the device and is not related to the network accessed by the user.