TELXESS
Consulting Services Pvt. Ltd

Dated: 12th March, 2017

Mr. Asit Kadayan
Advisor (QoS)
Telecom Regulatory Authority of India
Mahanagar DoorSanchar Nigam
Old Minto Road,
NEW DELHI – 110002.

Dear Mr. Kadayan,

Subject: Response to TRAI CP on Net Neutrality

We thank you for the opportunity provided by the Consultation Paper on the given subject matter and are happy to provide our response as under:

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

Ans: *In keeping with the Fundamental Right to Freedom of Speech and Expression, enshrined in the Indian Constitution, as also the fact that Access to Internet is the key means by which individuals can exercise their Right to Freedom and Expression and is an indispensable tool to realize a range of human rights, combating inequality and accelerating development and human progress (as stated by Frank La Rue, UN Special Rapporteur's to UNHRC), as well as the fact that Internet Services Licenses prescribe the scope of Internet Service as…'subscribers to be provided unrestricted access to all content on the Internet…, accept as restricted by the Licensor/law; the following General Open Internet Principles may be recommended and adopted for India:*

a. *All users, in India, shall have the right to create, access, receive, use, distribute and share all content, information, expressions, opinions, applications and services online by using any terminal or end user device connected to the Internet, as they wish, without any let or hindrances, interference or discrimination of any kind.*
b. *End user rights as in (a) above shall not be restricted except only to the*

extent that any particular online content and/or information is lawfully debarred/blocked or for any reason that a Court of Law may order debarment of any content.

c. *ISPs/TSPs/VNOs or any other online Service Provider shall not monitor, and or filter any traffic for the purpose of discriminating, in any way, or to interfere, block or alter, restrict, degrade, hinder or use any such practice or procedure that leads to throttling and/or improperly channelize, favorably prioritize as a means of favor to hinder competition, or impart any preferential treatment to any traffic or part of the traffic/content on the Internet which is otherwise publically accessible by users, running on the ISP/TSP/VNO's own or any affiliates network.*
d. *Network Neutrality is important to enhance the Network Effect, whereby; the value of any service or application will not be artificially diminished by any service provider through throttling or degrading the availability of that particular app or service, in keeping with the principles of Metcalf's law which states that, "the Utility Value of app increases with increase in the square of number of users".*
e. *Exceptions to the restrictions on ISPs/TSPs/VNOs as in (c) above shall only apply to the practice of exigent or justifiable traffic and network management, as may be prescribed by the Regulator, such that is necessary to ensure stable, unhindered operations and availability of services, removal of network congestion (without indulging in practices like fake clogging of ports), ensure security and integrity of network and services, or where such measures like monitoring and/or blocking are demanded in compliance of law specifically.*

We recommend that TRAI lay down a 'principles based non-justifiable/non acceptable set of TMP practices that shall not be allowed by ISPs/TSPs/VNOs, as well as a list of exigent, justifiable and therefore acceptable TMP practices. Both sets of allowable and non allowable practices is necessary, so as to remove room for doubts or misinterpretations.

Further, ISPs/TSP's/VNO's may be mandated to provide a public disclosure on their websites, whether or not they employ any ITMPs (Internet traffic management practices) and if they do, specifically mention the type, reason and duration for which the specific exigent ITMP is being employed. This disclosure may be added into the ISP-Customer Agreement for services, where obligations of both the ISP/TSP and customers is laid out.

However, to be fair, the General restrictions on TMPs may specifically be made

non –applicable for services such as Enterprise Networks involving Closed User Groups, where to gain QoS, enterprises use dedicated leased lines/fiber connections with SLAs, and where these Enterprise Networks do not fall within the purview of publicly accessible Internet.

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

(a) **Should certain types of specialized services, enterprise solutions, Internet of Things, etc. be excluded from its scope? How should such terms be defined?**

Ans (a): *Enterprises for their solutions requirements namely Managed services/CUG/Intranets and VPN's enter into SLA's with their service providers, to ensure negotiated QoS levels, for which they deploy dedicated leased lines or high bandwidth fiber connections or wireless or hybrid connections and architect their network infrastructure in a way as to ensure smoother flow of traffic. They use IP but are largely single networks with access restrictions and have no effect on the general accessibility of Internet by the public. Therefore, it is prudent, practical and necessary to keep Enterprise solutions out of NN purview.*

However, with Internet of Things, where machine to machine data transfer between devices is the key, experts in the field suggest that data transfer rates are not likely to be high enough any time soon and hence, discriminatory flow of traffic is not seen as a requirement in practice and therefore Net Neutrality does not pose any hindrance to development of IoT at this point. According to Machnation (an IoT Research firm) and other experts, IoT solutions and devices do not generate lot of data and so in the context of bandwidth and speed, there is no need for creating 'fast lanes' for IoT, making it unnecessary to make any specific provisions for IoT type of services in the foreseeable future.
In short Enterprise solutions/CUG/VPNs networks, where there is no public access to Internet at large and where specific SLAs are a pre-necessity, NN principles need not be applied. In the context of Internet of Things, NN does not pose any issues and general NN provisions default will apply either way. This can continue till such time as any specific issues emerge and to that extent the matter can be dealt with appropriately at that time.

(b) How should services provided by content delivery networks and direct interconnection arrangements be treated? Please provide reasons.

Ans (b): *CDN's are more a form of local content storage enabling more and more content to be placed closer to the edge of the network (and therefore closer to the user). Google, Facebook, Netflix, Akamai's and such others are examples of CDN's that enable content to be quickly delivered and available to the end users. These CDN companies typically have 'peering or interconnection arrangements' with the ISP's and the content is stored with the ISP, rather then travelling all over long distances across the Internet backbone. To this extent, Internet architecture has evolved and these CDN's cant be said to violate NN principles. CDN's do provide better Quality of Experience through their direct interconnection arrangements with ISP's, as these arrangements are becoming more of a norm than exceptions. For example imagine the experience of watching a Netflix movie if accessed from some US site vis z viz accessed from their local Indian presence. Violation of NN principles will be if ISP/TSP agrees for Netflix or Youtube, etc. to get a faster lane on the last mile to the customer and slow down or block other competing services on that network. Hence, while CDNs placing their servers at the ISPs PoP is acceptable, they may be debarred from any backdoor arrangement to discriminate against any other competing CDN or content, which may not have an agreement with the ISP.*

Another example is of Internet Exchange Points (IXPs), which are established the world over to ensure that content on the Internet is accessed and reaches users with less delay or latency or jitter as possible, since internet traffic from the source to destination will traverse less distance. Purely in technical essence this is traffic engineering. ISPs interconnecting/peering and CDNs and content providers inter-connecting with ISPs in the IXP facilities is a common feature all over the world and is being encouraged as well. (The author of this response first propagated and spearheaded the setting up of IXPs in India, as a result of which NIXI came up and hence has an understanding of the issue at hand).

What would violate NN principles is when the ISP's/TSP's with which the CDN's have a peering or an interconnection agreement, starts giving preferential treatment to the traffic of these CDN's, to the detriment of other's traffic, which can be done by introducing fake congestion, throttling or degrading the speeds of the other rival service providers. Netflix and Comcast agreement, which was challenged, is a known example from the USA, where Comcast (ISP) had to specifically confirm publicly that the agreement 'does not' include any provision for faster lane for Netflix (CDN).

Essentially, the overarching Aim of NN will have to be to prevent ISPs/TSPs

(especially the bigger/dominant ones more so – even though equally applicable to smaller ISPs as well) from becoming the content Gatekeepers, who by virtue of their legitimate interconnection or peering agreements with CDNs, should not get to decide which content get's on the net, which one moves slow and which moves faster. All lawful content should be equally free to be published, uploaded, and downloaded by any user without being policed by the ISP/TSP, as an essential feature to maintain the Open Internet. ISPs job is to ensure that end users have unfettered access to all content on the Internet.

Given, this principle we recommended that TRAI ask for ISPs/TSPs to provide Internet Traffic Management Policy Disclosure statement stating (in simple consumer understandable language), eg. type of traffic/content/protocol they manage/when and if so why, blocking being done and if so why, monitoring and why, deploying/not deploying DPI and if so why, if restricting P2P traffic and why, etc. As mentioned earlier, these disclosures could be published on SP's website and/or be part of the ISP/TSP-Customer Agreements and copies filed along with Tariff filings.

Additionally their interconnection and/or peering agreements copies may be filed with it (Regulator may consider allowing redaction of commercial pricing part to ensure business confidentiality) and in case of any perceived or real violation, Regulator can seek more information, assess, prescribe or take suitable remedial measures.
This is essential in India, where close to 98% of Internet traffic flows through only top 10 ISPs, most of whom are also the biggest TSPs and upstream carriers, indicating a relative concentration of power in the hands of a few Service Providers, with a large number of very small ISPs whose customers could be effected by their upstream Provider's ITMPs.

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

Ans: *Essentially both practice/s ie. Identifying justifiable TMPs as well as drawing an illustrative negative list is essential, to establish the operative principles to be followed in the true spirit and principles of Net Neutrality. It would also help in providing certainty and remove scope of misinterpretation and much ambiguity.*

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

Ans(a): Examples of reasonable ITMPs (which are already being used globally and commonly) would include practices to Limit, control, filter or mitigate effects of Undesirable Traffic such as Spam, virus, malware, and other malicious and security threatening traffic such as DoS attacks, etc. This would be essential in terms of fighting cyber crimes and needs to be acceptable.

Others examples may be some Prioritization techniques to ensure that during peak traffic times, to avoid congestion related delays, latency or jitter, Time Sensitive traffic/Real Time Traffic packets viz. Web Browsers, IMs, Video Conferencing, streaming multi-media, VOIP, Online Gaming etc.), are given Queuing priority or reallocated more bandwidth as compared to non real time, less time sensitive traffic such as Emails, software updates.
This could be acceptable during periods of traffic congestion (congestion or peak traffic periods are already monitored and known to the ISP/TSP).
However, while management of congestion of networks may be acceptable under certain strict conditions as mentioned above, it should not be used to mask or cover for under provisioning of network resources such as backhaul capacity/bandwidth, which is often the real reason for traffic bottlenecks in the first place as per most technical studies.

Additionally, filtering or blocking of specific content by way of lawful government or Court ordered instructions would have to be within permissible ITMP/Traffic Engineering Practices.

Ans (b) **Identifying a negative list of non-reasonable TMPs (the narrow approach). Please provide reasons.**

Ans (b): Examples of negative/non acceptable practices may include usage of tools such as DPI, to monitor type and actual content of the traffic or collecting and analysing personal information or browsing habits of users with a view to set up traffic management (policing) policies for or against some of the traffic, to restrict/block certain traffic like P2P, file sharing applications, block a rivals content or give priority to one's own or affiliates traffic for any commercial or non commercial reason or introducing artificial congestion with the intent to degrade any particularly targeted content/traffic, which the ISP/TSP may dislike for any reason (other than legally bound to do so).

Given the enormity of understanding required and implications on the way Internet is used or will be used in coming times, where different ITMPs may be applicable, not applicable and/or applicable selectively or in limits, based on type and class of

services, we recommend that a standing study group or a neutral task force (Open Internet Task Force – OITF) may be set up by TRAI, with experts (and representation from stakeholders) to study and create a set of Principles and Guidelines for Internet Traffic Management Practices/Traffic Engineering Practices/Traffic Shaping Practices for the Indian telecom/ISP industry and which will keep in line with various applicable legal provisions. For more detailed mandate for an OITF, please see our response to Question 12. The OITF can set out Guidelines with the provision to be reviewed and updated, periodically, from time to time as Internet keeps evolving.

Q.4 If a broad regulatory approach, as suggested in Q3, is to be followed.

(a)What should be regarded as reasonable TMPs and how should different categories of traffic be objectively defined from a technical point of view for this purpose?

Ans (a): *Broadly different categories of traffic types would be:*

- *(i) Non Real Time (P2P/Email/uploads/downloads),*
- *(ii) Time Sensitive (Online Gaming, VOIP, Video Conferencing),*
- *(iii) Interactive or Real Time (Web Browsing/Online shopping/Streaming/Chatting) and*
- *(iv) Undesirable Traffic (Spam/Malware/Worms/Botnets).*

While in general, it must be mandated that all types of traffic shall be treated identically, with exceptions to manage 'congestion', Blocking spam/malware traffic through firewalls, IPS, filters, rate limiting, black-holing, etc. to guard against or mitigate security threats such as DoS attacks, etc, are examples of TMP that have to be accepted policy and practice.

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

Ans (b): *In order to ensure that NN principles are followed in letter and spirit, some applications may be more prone to manipulation and discrimination by ISPs/TSPs, than others. For example, some TSP's/ISP's may prefer to have VOIP apps or OTT apps as undesirable and therefore choke or block the ports to degrade these apps, in order to protect their own legacy Voice or data service, or may want to charge more for the usage of these apps citing various reasons, or a ISP/TSP may have it's own/affiliate Messenger service given priority over a rivals*

IM app. These app level discriminations will be detrimental to consumer choice and cannot be allowed unless any application is determined to be harmful or cause harm to the network or to users of the networks (say a phishing apps or identity stealing apps, etc). In general, however, any other restrictions will destroy the essence of Internet of Open and Permission-less architecture.
ISP's/TSP's do however, provide different classes of services (low to high bandwidth services and charge as per the bandwidth size. This enables the customer to decide which class of bandwidth service is best for his type of applications usage and once he pays for the class of service, ISP/TSP then must remaim application agnostic – should have no role in deciding which application to give preference or not to give preference or which applications users can or cannot use).

However, apps that may be recognized as harmful (security threatening/law-breaking and such) to a network and its users need to be allowed for managed or dealt with under ITMPs appropriately.

© How should preferential treatment of particular content, activated by a users choice and without any arrangement between a TSP and content provider, be treated?

Ans ©: *Users adopt particular content or applications based on peer recommendations and reviews and popularity, driving the traffic up for that type of content. In that sense, content adoption does not require any permission from Network operators and ISP's. Popular example cited in most papers is about P2P file sharing using BitTorrent or similar, which as per some estimates drive a very large chunk of the global Internet traffic. Popular or otherwise, there may or may not be any commercial/non commercial arrangements between the content provider and the service providers. Irrespective of any arrangements, explicit or implicit, ISPs globally are known to slow down such P2P to prioritize other traffic, as per some declarations in some countries. We do not know the practice (not disclosed) in India and it is these practices that need even-handed regulation.*

Treatment of such arrangements needs to be part of our recommendation for making Disclosure statements of ISPs/TSPs and development of Principles and Guidelines for ITMP in India.

There are explicitly illegal content such as ones containing child pornography, protected IPR infringements, which will meet the requirement for targeted ITMPs.

As mentioned in our answer 3, we advocate adoption of a Set of Principles and Guidelines that we'll need to develop for both acceptable and non-acceptable ITMPs.
However, just to re-iterate, a task force (OITF as suggested) needs to be set up with a mandate to study global developments and practices by various regulators, TSPs, ISPs, Mobile operators, Content providers, and other stakeholders, Indian local laws and regulations and preferences which may be needed to take into account, based on which a time bound ITMP/TEC/TSP Set of Guidelines and Practices, reviewable periodically needs to be created and be adopted by the Indian industry.

Additionally, users download or subscribe to various security applications, such as firewalls, pc cleaners, blockers, anti virus, and other shields, which may in practice block or inhibit access to even some legitimate traffic. However, these practices, at the user level cannot be and should not be mandated against not is any regulation warranted.

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

Ans: *As we have stated in our Answers above, and as firm believers in Net Neutrality, we prefer a rational and realistic view with a balanced approach. We do not believe that realistically, either of the two extreme approaches i.e. Ban all discriminations or Allow all discriminations type of framework can work because it will be unreal and without basis.*

Overall, ITMPs that are intended or used deliberately or knowingly to block, filter, degrade, slow down or speed up or treat unequally or in any discriminatory manner, any or part of the traffic which is lawful, with the intent to give preference to competing own/affiliate or third party content and or traffic for any consideration, commercial or otherwise cannot be allowed, except where and when necessary to prioritize for congestion management, to block or filter out any traffic/content/app which is determined to be unlawful, malicious or harmful needs to be allowed.

But again we emphasize the need for a focused Study and Development of a Set of Principles and Guidelines which while completely protecting the principles of Net Neutrality (ensuring and guaranteeing the continued evolution of an Open Internet, ensure consumer trust and transparency), will simultaneously identify and mandate blocking of anti competitive and consumer detrimental actions where the

Service providers do not become gatekeepers; also recognize that certain technical and operational measures are already inherent in the nature of Internet access service provisioning and may have to be acceptable for better QoS (enhanced consumer access experience); or whether some of these prevalent practices need to be revisited and modified from time to time.

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

(a) **Emergency situations and services**;

Ans (a): *No specific conditions/exceptions are warranted for Emergency situations or services.*

First, in India, given the situation that major parts of the country are not even connected to the Internet, it is more important that Internet infrastructure becomes more widely available, for masses to be able to rely on it's potential supremacy as a resilient and dependable communication network for emergencies, such as setting up of ad hoc networks in disaster areas.
Secondly, there are different types of emergencies and phases of emergency (mitigation, preparedness, response and recovery), where each situation warrants different communications and information plans and network needs. Hence, it's not practical to think in terms of ITMPs, with regards to Emergencies in general terms.

Third, National Disaster Management Authority, have in its plan mentioned requirements for a dedicated and reliable (wrt bandwidth) nationwide NDCN (National Disaster Communication Network), with last mile networks based on satellite and VHF links, with evolution towards Wi-Fi/Wimax links and go on to list various other complex requirements. This type of network will ensure it's own resiliency when built.
Therefore, in the absence of any specific co-relation to standards or requirement from specialized agencies like NDMA, NDRF, DDMAs, etc., it'll be futile to consider any unilateral ITMP measures. They have laid out a complex design and architecture plan, utilizing different technologies, for a dedicated NDCN, with QoS inbuilt, on the lines of a large enterprise solution with it's own unique requirements.
Hence, there seems no immediate need to make specific provision now.

(b) Restrictions on unlawful content;

Ans (b): *License conditions already forbid and require Service Providers to take measures to prevent the flow of unlawful content. Additionally, Government already issues site and content blocking instructions that have to be complied with, without fail. To that extent, this exception to NN principles is an accepted measure and can only be subject to review or revision by courts of law, if challenged. Also, courts may take cognizance and order blocking of explicitly harmful content, which have to be necessarily complied with.*

Hence, either voluntarily under proper disclosures, or through lawful directions of government, through Court Orders, exception to prohibition on ITMPs will need to be allowed in cases involving unlawful content/traffic.

Also, as per License conditions, ISPs/TSPs are required to provision LIM tools, which may have the potential to be used for infringing upon the NN principles. However, these tools are to be used under the LEA's supervision and under their authority. It may suffice for operators to declare this arrangement in their disclosures.

(c) Maintaining security and integrity of the network;

Ans © : *As mentioned earlier, any malicious content/app/traffic or activity that is aimed at harming or has the potential to harm, interfere or disrupt the network or deny or deprive legitimate users the use of the networks and its services which they are entitled to, can be subjected to appropriate and proportionate ITMPs.*

(d) **Services that may be notified in public interest by the Government/ Authority, based on certain criteria; or**

(d) Any other services.

Ans (d): *No specific exceptions in terms of managing 'fast lanes' for specific services needs to be mandated. In principle all types of traffic (with exceptions of undesirable, unlawful, malicious and harmful types or for management of congestion) has to be treated equally and without discrimination.*
We have provided variety of reasons and examples throughout this response to support our contentions.

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:

(a) Blocking;

(b) Throttling (for example, how can it be established that a particular application is being throttled?); and

b) **Preferential treatment (for example, how can it be established that preferential treatment is being provided to a particular application?**).

Ans (a), (b): There are many different types of tools and tests that have been made available such as those by M-Labs, eg. Neubot, Pathload, Windrider, Network Diagnostic Tests, etc. to measure Network Performance, Transparency and Network State, etc. But these have been used in the context of Networks in the US, etc. and their test results are more related to those networks.

In the Indian context, specialised work is needed to look into the available tools, check their efficacy, or even develop more tools, put them to use and test the networks in different conditions over a period of time, obtain data and analyse in order to detect and establish instances of throttling, blocking or prioritising. Hence, again our suggested OITF (Open Internet Task Force) which can be set up and it mandated to develop the capacity to test networks for ITMP practices.

However, most simple test speeds which ordinary users use such as speed tests cannot be reliable (as these themselves can be manipulated – ISP may detect the speed test app and allow higher speed to ensure better readings) and hence may be of limited use only.

Q.8 Which of the following models of transparency would be preferred in the Indian con-text:

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

Ans (a): *Broadly the Information Disclosure Template sample provided in the CP is fine.*

However, Authority needs to clarify, for the sake of avoidance of doubts and ambiguity, what types of services would be covered under specialized services. Further, if specialized services relate to Enterprise Solutions, VPN, corporate networks, the terms of SLA's/guaranteed QoS entered into would be sensitive

business information and need not be disclosed publicly on any site. These agreements could be produced only if and when they are subject to regulatory or legal disputes.
With regards to all other's, there should also be an AUP (Acceptable Use Policy), which correspondingly states the customer's obligation or informs users of activities that they should not do and which would be construed to be illegal (where customers and users are warned from using or introducing unlawful, malicious content/apps/traffic into the network or intentionally tamper with/harm the network and its legitimate users or are offences under the IT Act or under the ISP License conditions).

(b) **Disclosures to the regulator**;

Ans (b): *ISPs/TSPs may provide copies of their ITMPs on the suggested Information Template.* Service Providers can *submit the Information template copy along with other quarterly reports submitted by them to the Regulator.*
Further, when the Task Force (OITF) designs and recommends the detailed Set of Principles and Guidelines for ITMPs, the Disclosures may state their general compliance to those Rules and any deviation that there may be.

(c) Disclosures to the general public; or

Ans © : *ISPs/TSPs will find that disclosing their adoption and compliance to a set of ITMP principles including use of Information Disclosure Template/AUP will result in improved transparency and trust between itself and the customers while enhancing credibility of ISPs/TSPs in the eyes of the stakeholders, public, regulators and the government. This may be displayed in customer understandable simple language, on their respective websites. Regulator may also post these submissions from Service Providers on the TRAI website.*

(d) A combination of the above.

Ans (d): *As is evident from our responses to (a), (b), (c), it is apparent that we recommend all round disclosures in the interest of transparency and improving trust and credibility between ISPs/TSP's and public at large.*
Except that specialized services such as Corporate Network, Enterprise solutions, VPN, need not be covered under these general category norms, since they have their specific business sensitive SLAs and guaranteed QoS agreements.

Please provide reasons. What should be the mode, trigger and frequency to publish such information?

Ans: *Consolidated ITMPs Disclosure template along with AUP and billing plans, etc. are in the nature of establishing a set of mutual obligations and responsibilities for the ISP/TSP and customers as well. This could be provided along with the customer sign on format (available to all customers with their online service accounts) and should remain applicable till the duration of customer service, unless modified/updated or amended.*

This disclosure format should be made available at the point of sales, whether online or offline (for the customer to be able to compare and make informed choices).
A standard current template should also be posted on the ISP/TSPs website as well as available on the customer's online service account page.
Service Provider's can file a copy with the Regulator along with other quarterly reports that are filed, unless a modified/updated version becomes necessary.
If and when a new version becomes necessary, the same could be be filed with the regulator, a few days prior/in advance to general dissemination.
The information can be modified appropriately in case of change of policies or practices that may happen over a period of time, for various reasons.

Q.9 **Please provide comments or suggestions on the Information Disclosure Template at Table 5.1? Should this vary for each category of stakeholders identified above? Please provide reasons for any suggested changes.**

Ans (9): *As mentioned by us above, the IDT should also include a Acceptable Use Policy for customers, contained within the template, laying out activities (undesirable/unlawful/malicious activities/constituting offences under IT Act or License Guidelines) which customers are required to desist from.*
The reason for the AUP, is to ensure that apart from the Service Providers obligations, Internet users should also be aware that there are certain activities that are not acceptable or barred by law, and since breach of these obligations by users may have legal implications they have to be assume and accept responsibility towards any intentional illegal use and harming of the network and services.

We see this as a standard Disclosure format and should be applicable to all types of Internet access customers, barring those that have individual enterprise SLA's which may be subject to general non-disclosure norms (unless demanded under law pertaining to any legal/regulatory dispute).

However, the Standard format information needs to be also calibrated according to the class and technology of services provided. For example, the details will be different for mobile based 2G/3G/4G/LTE services, or in case of DSL based service where, characteristics and performance will vary based on the speed plus bandwidth packages that customer's opt for.
The formats will need modifications from time to time, based on changes in service/tariff conditions, which can be informed by Service Providers to the regulator, prior to being made available publicly, just as it is done in case of advance tariff filing.

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?

Ans: *As we have suggested, a Open Internet Task Force (OITF) for creating the Principles and Guidelines for ITMPs needs to be set up. This Task force should be a Standing body, which after introducing the ITMPs Principles and Guidelines, can be charged with monitoring it's implementation, receiving public inputs on perceived and/or real violations, analyse reported violations based on validated complaints , or suo moto, and recommend appropriate remedies, keep abreast of developments, globally as well as locally, conduct surveys and audits of the networks and plan for adopting future policies and practices and also support development of network and performance measurement tools and techniques to test and establish illegal blocking, throttling or prioritising practices.*
If found the NN Guidelines violated, it could also be tasked for recommending the type and extent of penalties, which may be suitable for adoption by TRAI, as a sub set of it's financial disincentive levies.

(b) **What actions should such body be empowered to take in case of any detected violation?**

Ans (b): As mentioned in answer above the standing body OITF needs to take cognizance of complaints and feedbacks on a regular basis, analyze the inputs, seek responses from Service Providers and if found appropriate initiate and conduct tests and measurements with available tools of the suspect network. In case proof is found of violations, depending upon the nature and intensity of the violations and its effect or damage it may or could have caused to users or to other networks and it's users because of degraded QoS, the Body can recommend

proportionate penalties under a set of financial disincentive levies, which would be appropriate to deal with NN violations.

(c) **If the Authority opts for QoS regulation on this subject, what should be the scope of such regulations?**

Ans © *As mentioned above, we are recommending setting up of the OITF, which can look into the QoS framework and recommend to the Authority appropriately.*

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).**

Ans 11: *Kindly see our response to Question 7, which mentions the type of tests to monitor are available but may have limitations in the Indian context. Hence, we are suggesting the setting up a specialised body, the OITF (also see our response at Question 12), which suggests the setting up of OITF again, under the aegis of TRAI itself and dedicated to the task of keeping abreast of developments, issues, analyzing complaints, receiving feedback, reports and complaints, collating and disseminating information, recommending actions and generally being in-charge of ensuring that any extant NN guidelines/ITMP principles and practices are followed in letter and spirit.*

Q.12 Can we consider adopting a collaborative mechanism, with representation from TSPs, content providers, consumer groups and other stakeholders, for managing the operational aspects of any NN framework?

(a) What should be its design and functions?

Ans (a): *We are recommending that a neutral body viz. Open Internet Task Force*

(OITF) be set up, comprising of subject matter experts, with representation from stakeholders, which will:

(i) *Study global NN norms and practices and provide a time bound ITMPs Principles and Guidelines, which they can introduce for adoption.*

(ii) *The Open Internet Task Force can become a Standing Body which can then be charged with monitoring implementation of ITMPs Guidelines,*

(iii) *Receive public inputs, complaints, feedback on violations,*

(iv) *Conduct analyses of such reported violations and recommending appropriate remedies to Service Providers and to the complainants,*

(v) *Keep abreast of developments, globally as well as locally; conduct surveys and audits of the networks and planning future policies and practices.*

(vi) *Commission research and development and use of reliable tools and tests to detect instances of throttling, blocking of lawful traffic and establish veracity of illegal prioritizing of traffic.*

(vii) *In addition, it could also be tasked for recommending the type and extent of penalties, which may be suitable for adoption by TRAI, under it's set of financial disincentive levies.*

(viii) *It may also create a plan for regular public awareness campaigns with regards to the rights and obligations of both Service Providers and Users, in the context of NN, as also support publication of opinions, articles, documents related to the subject of NN.*

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

Ans (b): *The Standing Body on ITMPs may function under the aegis and overall supervision of TRAI and funded by it. Alternatively, funding for OITF can be arranged from USOF.*

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?

Ans (13) : *We strongly recommend a Open Internet Task Force as outlined in our Answer to Question 12 and earlier responses. This body supported by TRAI may ensure that developments are kept pace with and suitable policy and regulatory*

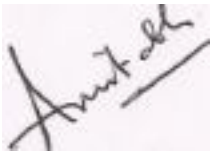
recommendations are made from time to time. It is essential considering that Internet is still evolving and pace of change is rapid and lagging behind will not be desirable.

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?

Ans (14): *Please see our Ans 12 (viii) to Question 12 (a), where the solution would be to have the Open Internet Task Force which monitors, develops recommendations and help implement the NN principles.*
Pubic awareness through reliable publications and journals on various developments and aspects of NN is a step to educate the public, community and stakeholders, so as to ensure that all become sufficiently aware of the realities of NN and how it works even from an individual users context. In addition of course, we believe that Service Providers too will play a role in educating the public over time as adverse public perception about the services impacts the Providers as well.

Thank you again for the opportunity to put in our views and look forward to the Authority's actions on the matter.

Sincerely
For Telxess Consulting Services Private Ltd.



Amitabh Singhal
(Director)

Registered Office: C-73, Upkar Apartments, Mayur Vihar Phase-I, Extn, Delhi – 110091. Telephone: +919810081774. Email: Amitabh@amitabhsinghal.in