Annexure-I

PREAMBLE

Nokia is a global leader and continues to be, an innovation leader in the technologies of communication that connect people. Nokia is playing a leading role in shaping the new revolution in connectivity and digitization, where everyone, everything, everywhere are connecting.

Nokia is also pursuing new ways to converge network and deploy the new technologies that that are shaping the future of the connected world: 5G ecosystems, Cloud-based networks, IP routing, Optical fiber transport, Internet of things and Data analytics and creating opportunities for our customers (Service providers, Enterprises, Governments) and new experience possibilities for end users of our technology.

Nokia is ready to meet the huge demand on network performance and access for which there is a need to simplify, optimize, and automate the complex flow of data across the network, data and technology to enrich our lives.

Nokia fully supports the digital India vision of the government and promoting ecosystem which enables fulfillment of this vision.

Keeping in view the great complexity of technical, economic and policy-related issues that Net Neutrality involves, pinning down a precise definition of net neutrality is difficult. One of the most balanced perspectives in defining Net Neutrality is as given below:

"No denial of access and absence of unreasonable discrimination on the part of network operators in transmitting internet traffic."

Issue of Net Neutrality is a complex issue that is being debated in several countries all over the world and administrations are looking for the right solution to ensure the continued growth of the internet whilst managing the unique challenges of a mobile environment, where capacity is finite due to limited availability of spectrum and huge investments are required to sustain the growth of internet traffic. Operators have to manage their resources and capacity to ensure the best possible customer experience.

Net Neutrality should be looked at from the holistic framework of Internet Governance. There are multiple approaches to look at net neutrality.

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?

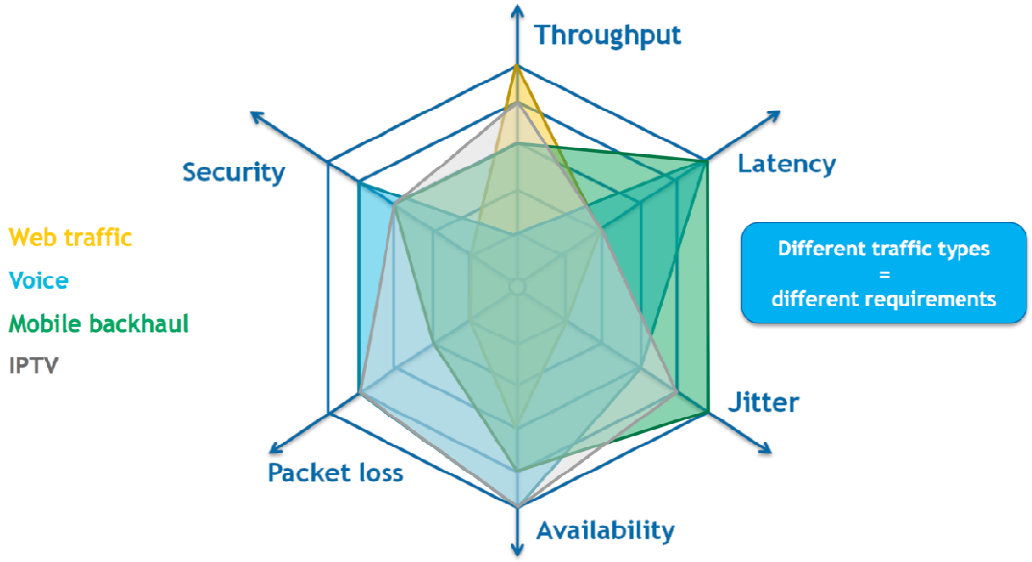
End-users should have the right to access any legal content, service and application of their choice via their Internet access service. This is the basic principle of the open Internet and net neutrality.

The notion that all traffic is treated equal does not guarantee this right. Rather, if implemented into law it would effectively make it impossible to deliver the best effort Internet where networks are managed to ensure to the greatest extent possible that the right packets are delivered to the right place at the right time.

Consequently, a definition of net neutrality that would embed a principle that 'traffic should be treated equally' is not necessary and should not be in the text. Such a principle could ultimately undermine the overall objective of the Regulation by deteriorating end-users Internet experience.

Not all bits are created equal: different types of traffic have different requirements.

When different packets arrive at a router at the same time and there is congestion, some packets will be momentarily dropped. They will automatically try again in a few milliseconds. However, if the packet is for a VoIP service, the delay may distort the image or sound, negatively affecting the end-user experience. If the packet is for an email, a short delay of a second will not cause any negative impact to the recipient of the email.



This is why different types of data are given different kinds of treatment and why implementing a principle that all data is equal would deteriorate our Internet experience. For more info, see video on how the Internet works: https://www.youtube.com/watch?v=ZonvMhT5c_Q.

Reasonable traffic management plays a fundamental role in ensuring a good end- user experience with the increasing Internet traffic and is an integral part of network management. While operators should not be permitted to block, throttle, degrade or otherwise apply anti-competitive measures against specific content, applications or services, traffic management is not in itself anti-competitive.

Humans generate not all web traffic. Software agents generate in fact more web traffic than humans. They are shaping our online experience by influencing the way we interact, learn, trade and work. Many of them are used for malicious activity (spam schemes, DDoS floods, mass-scale hack attacks, click fraud campaigns...) that impacts significantly our activities

online. Traffic management is essential in maintaining a consistent user experience and minimise the business and financial impacts on companies in the case of mischief.

Reasonable traffic management should be permitted to ensure that the day-to-day delivery of best effort Internet can be maintained while there are clear protections against bad behaviour. The terms for reasonable need to be clear, i.e. transparent, proportionate, non-discriminatory and not anti-competitive. As non-discriminatory can be interpreted in different ways the text should in particular make clear that non-discriminatory does not prevent operators from treating different types of traffic differently in accordance with their technical requirements.

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?

Traffic management is a vital means to provide efficient, effective and safe internet access services as well as other services to meet different needs and types of use with varying and flexible quality levels.

By other services, we mean services which are designed for specific content, applications or services, or a combination thereof. Such services rely on traffic management or other networking techniques to ensure the desired or necessary level of network resources that determine subscriber experience (such as capacity, quality) with the aim to securing enhanced quality characteristics. They are delivered from end-to-end and are not marketed or widely used as a substitute for Internet access services.

The voluntary code of practice on traffic management transparency for broadband services published in May 2013 by the Broadband Stakeholder Group in UK gives an overview of what traffic management is:

“Traffic management is a component of an ISP’s overall approach to network management. Network management includes elements such as capacity planning and network dimensioning to provide a quality of experience for [customers]. Traffic management practices are subsequently used to deliver and maintain that experience for [customers].”

Traffic management can only be done in the infrastructure domain the operator controls and is required to operate, administer and maintain it.

Traffic management measures are necessary in particular to:

- prioritise time-critical applications (voice, video, emergency notification) – since best effort delivery does not provide any time and bitrate predictability
- preserve the integrity and security of the network, services provided via this network, and the end-users' devices
- protect the network from overload conditions

The main network traffic management use cases have been documented by the Broadband Forum organisation in the Broadband Policy Control Framework (BPCF) Technical Report

TR-134 Corrigendum 1 (https://www.broadband-forum.org/technical/download/TR-134_Corrigendum-1.pdf).

Traffic management is a key to prevent congestion for:

- load balancing of flows in the network to improve the overall resource usage while avoiding local traffic bottlenecks when possible, and
- admission control prior to the admittance of new flows in order to avoid that running services suffer from a lack of bandwidth if new flows arrive while the remaining available physical or logical bandwidth are not sufficient.

It is also important to allow TSPs to optimise traffic management when congestion occurs to:

- treat flows having a higher priority prior to other flows,
- re-route flows to reduce local congestion, etc.

The Broadband Forum organisation has defined the congestion point as: “A physical or logical egress point in the network where the sum of aggregated ingress traffic can be larger than available physical or logical bandwidth. Physical congestion points include Ethernet ports and DSL local loops. Logical congestion points include ATM VCs, ATM VPs, Ethernet VLANs, Ethernet SVLANs and MPLS LSPs”.

Non-exhaustive congestion management tasks:

- When a server denies further sessions once a certain number had been reached or once a user has reached the number of sessions for his contract (video on demand, cloud services, VoIP lines...)
- When the network denies access to a user for new requests in a given (e.g. metropolitan) area, as the number of simultaneous users is already high and use the available bandwidth (e.g. refusing new video on demand sessions during busy hours). Compare to the previous point, the limitation is not at the server side or from the user contract but at the network level.
- When a household broadband connection is under dimensioned for the number of services requested (correlated to the number of family members and devices connected)
- When a household is dependent on WiFi spectrum availability especially in densely populated areas
- When the network operator notifies that an application requests more TCP streams than required to secure bandwidth over other applications
- When monthly traffic has exceeded the volume cap(s) defined in the user contract, some packets could be dropped

Preventing congestion and optimising traffic management when congestion occurs are part of the traffic management tools applied at all time on a network.

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

The policy and/or regulatory approach should apply to consumers and businesses and cover Internet Access Service, traffic management and transparency requirements:

- Internet Access Service would ensure for consumers and businesses access to the Open Internet based on best effort (unpredictable bitrate, unpredictable time): the right to access and distribute content, the right to use and provide applications and services and the right to use terminal equipments of their choice
- Traffic management is vital. It is about how networks are configured to enable the most efficient use of network resources and to increase overall transmission and throughput rates for the different kinds of traffic.
    - The Regulation shall not contain any duration, timing or congestion-based conditions on when reasonable traffic management measures can be put in place. It is not something which is “switched on and off”.
    - There is no trade-off between capacity and traffic management as implicit in the draft guidelines. While investments into network capacity will be needed to support the exponential growth in IP traffic, more capacity will not reduce the need for traffic management, nor will it address latency, throughput and jitter needs for services and applications.
    - With digitisation and IoT, networks will become more complex as they will be supporting a significantly wider range of services and applications. The technical requirements of packets will become increasingly heterogeneous and management of networks will consequently be imperative to enable delivery of all of these services according to their individual technical needs.
- Transparency requirements on TSPs to provide meaningful information (including in contracts) about the characteristics of the Internet Access Service and the reasonable traffic management measures.

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.

To preserve national security interests, TSPs should be allowed to restrict connectivity and/or block traffic:

- To preserve the integrity and security of the networks, and
- To comply with national legislation and orders by courts or other public authorities

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

To maintain customer privacy, TSPs and OTT service and content providers should fall under the same protection of privacy and personal data regulation, and not specifically to the electronic communication sector.

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

It is important to have a level-playing field between TSPs and OTT service and content providers.