CONSUMER PROTECTION ASSOCIATION

HIMMATNAGAR

DIST. SABARKANTHA

GUJARAT

Pre- Consultation Paper

on

Net Neutrality

Introduction :

Wireless mobile Internet is migrating toward an integrated system of Internet and Telecommunication Technology in order to fulfill the future telecommunication requirement. The open Internet drives the Indian economy and serves every day as a critical tool for Indian citizens to conduct commerce, communicate, educate, entertain and engage in the world around them. The benefits of an open Internet are undisputed. But it must remain open. Open for commerce, Innovation and speech, open for consumers and for the innovation created by application developers and content companies and open for expansion and investment by Broadband service providers.

Internet has become the vehicle of economic growth, social program delivery and governance in several countries. These aspects of internet are of critical importance to India, as they are too many other emerging economies. Studies have shown a direct impact of Internet growth on Gross Domestic Product (GDP). Recognizing the importance of Internet in all aspects of National and International trade, economy innovation and security, Internet Governance is increasingly becoming centre stage both at domestic and international levels. It is expected that such issues will become center stage as a part of Global diplomacy in the similar vein as climate change.

According to the Ericsson Mobility Report India edition, the number of mobile subscriptions in India will touch 1.37 billion by 2021. The report, which shows key trends on mobile traffic, subscriptions, consumer behavior and technology uptake specific to India, forecasts that :

1. The usage of mobile broadband would increase dramatically with smart phone subscriptions growing four-fold to 810 million.
2. Total mobile traffic increasing 15-fold to 4.5 exabytes (EB) a month by 2021.
3. Data Traffic per active smart phone will rise five-fold from 1.4 GB a month in 2015 to 7 GB a month by 2021.

4. By that year, 99 per cent of the region's mobile traffic will be from data.
5. The report says that smart phone users in India rate data as more important than voice, indicating the strong uptake of data services in the country. Data speed is considered to be the most important factor in determining the network performance and smart phone users' satisfaction with their operators.

It's the young smart phone users between 15 and 24 years of age who drive the need for better data speed and data coverage. These users also have a higher inclination to pay a premium for such services, the report notes.

STRONG SIGNAL

- **810 mn:** The usage of mobile broadband would increase dramatically with smart phone subscriptions growing fourfold to 810 mn
- **15 times:** Total mobile traffic would increase 15-fold to 4.5 exabytes a month by 2021
- **5 times:** Data traffic per active smart phone will rise five-fold from 1.4 GB a month in 2015 to 7 GB a month by 2021
- **99%:** By 2021, 99% of the region's mobile traffic will be from data

As per Cisco Visual Networking Index complete forecast for 2015 to 2020 Internet of Things (IoT) will continue to drive IP traffic globally. Applications such as video surveillance, smart meters, digital health monitors and a host of other M2M services are creating new network requirements and incremental traffic increases.

As per the forecast, any capacity constrains being faced on account of increased user traffic, will eventually have to be addressed through an overall improvement in the network infrastructure.

Carefully tailored rules to protect internet openness will allow investment and innovation to continue to flourish and prevent specific practices which are harmful to internet openness blocking, throttling and prioritization as well as a strong standard of conduct designed to prevent the deployment of new practices that would harm internet openness. TRAI should also enhance transparency rule to ensure that consumers are fully informed as to whether the services they purchase are delivering what they expect.

Rules on net neutrality are necessary to protect innovations on the internet and to preserve the kind of openness that have allowed the internet to flourish. Without rules ISPs will change their price structure to tired systems with the highest level services out of the financial reach of many enterprises wishing to start their own internet business.

In the absence of a clear regulatory framework on net neutrality, advanced traffic management techniques can potentially be used by an operator for discrimination or anticompetitive purposes.

COMMENTS :

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?

The approach to deal with emergent issue in Internet Governance requires flexibility, ability to incorporate new technologies and International development.

The role of Internet in economic growth and social aspects has increased the importance of Internet Governance. Internet Governance covers a wide gamut of resources and Institutions at National, Regional and International levels. Owing to the distributed architecture of the internet wide variety of issues that span internet governance and the high need for co-ordination and consequent adoption of Universally accepted protocols, National and International organizations play a role.

Net Neutrality : Definition :

All traffic on the internet should be treated equally. The service provider should not block or slowdown the services on applications we use over the web. The Internet service provider whether it is a

cable company of Telephone service can't create so called fast lanes that force content companies to pay additional fee to deliver their content to customer faster.

There should be :

1. No blocking :

A Service provider should not block lawful content, applications, services or non harmful device.

2. No Throttling :

Service providers should not slowdown specific applications or services, a practice known as throttling. More to the point, the service providers should not single out internet traffic based on :

(a) Who sends it
(b) where it is going
(c) What the content happens to be or
(d) whether that content competes with the provider's business

Telecom Service providers should treat all internet traffic on an equal basis, without regard to the : - Type
- Origin or
- Destination

Of the content or the means of its transmission.

3. No paid prioritization :

A Service provider should not accept fees either in cash or kind for favored treatment.

4. Reasonable Transparency

The Principles :

1. Send and receive all lawful content
2. Use all lawful services and applications
3. Use all lawful devices that do not damage the network.
4. Access all network, service, content and application providers.

The principles should also ensure ISPs :

5. Do not discriminate against lawful content services, applications or devices
6. Reveal any practices that could limit the previous five principles.

In short, all points of the network should be able to seamlessly connect to all other points, without any discrimination on the basis of speed, access or price with transparency.

The Government's policy stance on net neutrality must adhere to the following six core principles:

(i) User is the king and user's choice cannot be compromised. However, the interests of future generation of internet users cannot be compromised for short term interests of the current generation of internet users.

(ii) Same type of services should be subject to same threshold of regulations.

(iii) There should be no blocking, no throttling or inexplicable slowing down of lawful sites/services/applications by network intermediaries.

(iv) There should be no conflict of interest between content carrier and content provider with respect to internet based services.

(v) Providers of internet based services should be transparent with respect to their pricing models and operations.

(vi) Providers of internet based services should be held accountable for the 'Quality of Service' promised by them to their customers.

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?

1. Network operators should disclose information on differential treatment of traffic. We recommend transparency when it comes to the practices used to implement the differential treatment of Internet traffic. Specifically with respect to consumer-facing services such as mass-market Internet access, network operators should disclose the use of traffic differentiation practices that impact an end user's Internet access service. The disclosure should be readily accessible to the public (e.g. via a webpage) and describe the practice with its impact to end users and expected benefits in terms meaningful to end users. The disclosure should include any differentiation amongst Internet traffic and should disclose the

extent and manner in which other services offered over the same end user access facilities (for example video services) may affect the performance of the Internet access service.

2. Quality of Service metrics should be interpreted in the context of Quality of Experience. Common Quality of Service metrics, often included in commercial service level agreements, include throughput, delay, delay variation, and loss, among other things

3. The key parameters which impact users are delay; delay variation and information loss. Which need to be minimize. For this purpose various types of traffic can be classified. Some classes are error tolerant and some are not. The traffic in each class can tolerate only certain delay, jitter and packet loss characteristics. Therefore, the priority and QoS have to be attributed accordingly with highest priority to voice and video traffic and lowest priority to non-critical background services. Therefore, it is necessary to distinguish the different types and treat them accordingly.

4. The following are few categories into which the traffic management implementation may be classified :

4.1. Differentiation : It is the practice of treating different types of traffic differently.

4.2. Maintain the security and integrity of network from undesirable attacks.

4.3. Congestion control : The type of control can be either application agnostic (i.e. treat all IP traffic in the same manner) or Application specific congestion control (e.g. sparing the time sensitive applications and performing congestion control on time in sensitive applications) within the " Internet traffic " class may be against the principles of Net Neutrality.

5. From a user's perceptive, performance needs to be expressed by parameters which focus on user perceivable effects, rather than their causes within the network; are independent of the networks internal design; take into account all aspects of the service from the user's point ; can be assured to a user by the service provider(s).

6. There are many methods to manage as well as audit the service provider's network traffic. Traffic management methods have been continuously evolving. Some of the more popular methods are QoS (Quality of Service), DPI (Deep packet inspection), data volume caps, setting consumer broadband connection speed etc.. "QoS" and "DPI" are network management practices but " data volume caps " and " Setting consumer broadband speeds " are business practices. **From a Net Neutrality perspective QoS and DPI are important.**

7. TSPs/ISPs may not always treat the network traffic in neutral way. Some traffic management methods could also be used to derive some undue advantage without reasonable justification. Such practices will then have implications for net neutrality and so need to be regulated.

8. Illegitimate traffic management techniques could lead to discrimination by fixed or mobile TSPs/ISPs with market power in favor of their own applications, contents and services, thus harming both competition and consumers. Therefore, when traditional fixed/mobile operators are also functioning as ISPs, they may have a tendency to block or slow down the VoIP traffic of competing ISPs.

9. When TSP/ISPs start blocking/throttling of competing applications/ services from different content providers, or prioritize certain traffic based on exclusive arrangements, the incentive to develop new and innovative applications and services by the other content providers goes down. Start-ups will have a difficult time to establish their business. Without the cash flow that major companies enjoy, start-ups might not be able to afford the fees necessary to deliver content to customers. Telecommunication companies can pick their preferred partners, subsidize the data costs for their apps, and make it much harder for new entrants to compete with the incumbents. This will be detrimental to innovation.

10. Discrimination may lead to degradation of quality of service. Mainly two types of degradation of quality of service may occur :

10.1 Internet access service as a whole - (e.g. caused by congestion on a regular basis). This happens because, when traffic is throttled / blocked by the TSP/ISPs, there is a ripple effect on the routers where traffic starts piling up as the IP packets are not cleared as fast as they are arriving. This leads to artificial network congestion.

10.2 Individual applications - VoIP, VoD and sometimes sensitive P2P applications (e.g. video call on Instant Messenger) services get degraded in quality because they are very time sensitive.

11. Unreasonable traffic management also puts users at disadvantage. For example blocking of tethering applications on mobiles. Tethering application allows the customer to use the data connection to run Internet applications on another device, such as a laptop. Clearly, this allows many more opportunities to use innovative services on a phone. The main reason for constraining devices from 'tethering' is simply to extract more payments via a second contract. Yet a customer has paid for a certain amount of data within fair use limits already. There seems to be little reason to block the use of such applications, except to exploit the closed device to maximize

payments. While the means of managing traffic is through the device and its contract, rather than through packet management, this is considered a 'Net Neutrality' issue, as the network operator is using traffic management techniques to create unreasonable management of their network.

12. TSPs/ISPs should be mandated to make adequate disclosures to the users about their intervention practices to maintain transparency and allow users to make informed choices. It is also necessary for the regulator / government to lay down rules for disclosure and also for what practices can be allowed/disallowed, keeping in view the principles of Net Neutrality. A suitable grievance redressal mechanism is also required to be put in place.

13. Due to variety of traffic on the IP transport network, the concept of one size fits all does not work and differentiation becomes an essential function for network management. But many consider the use of traffic management tools as compromising the openness of the internet. There is a delicate balance between ensuring the openness of the Internet and reasonable and responsible use of traffic management by TSPs/ISPs for legitimate needs. Operators should be prohibited from practices considered as contrary to Net Neutrality principles.

14. Legitimate traffic management practices can be allowed but should be "tested" against the core principles of Net Neutrality.

15. General criteria against which these practices can be tested are as follows:

15.1 TSPs/ISPs should make adequate disclosures to the users about their traffic management policies, tools and intervention practices to maintain transparency and allow users to make informed choices.

15.2 Unreasonable traffic management, which is exploitative or anti-competitive in nature, should not be permitted.

15.3 In general, for legitimate network management, application-agnostic control may be used. However, application-specific control within the "Internet traffic" class should not be permitted.

15.4 Traffic management practices like DPI (Deep packet inspection) should not be used for unlawful access to the type and contents of an application in an IP packet.

15.5 Improper (paid or otherwise) prioritization should not be permitted.

15.6 Traffic management is complex and specialized field and enough capacity building needs to be done. Mechanism to minimize frivolous complaints desirable.

16. Some traffic management practices are regarded as " Un reasonable interferences with Internet traffic by a TSP ". This include :

16.1 Discriminatory traffic for data services based on the applications, websites or other content being accessed by the user, which has already been prohibited by the " Prohibition of Discriminatory Traffic for Data services Regulation, 2016 ".

16.2 Inspection of the contents of data packets, except to meet lawful requirements or to maintain the security of the network.

16.3 TSPs are not providing accurate information about Internet services offered to users to help them make informed decisions. TSPs should mentioned terms including aspects of bandwidth, price and the network management policies being enforced.

16.4 There should be no technology which classifies traffic by application and protocol and manages it by blocking, prioritizing, rerouting and assigning bandwidth.

16.5 There should not be user specific traffic management policies.

16.6 Policy and charging rules function software module which trigger user specific or group specific scenarios, traffic plans etc. should not be used.

16.7 The software like Jet subscriber manager (JMS) which discriminate tariff plans, connected services, network resources like channels loud applications priority, the user session status particularly traffic used etc. should not be used.

16.8 They should not block or slowdown access to video streaming services just because it thinks those services use too much bandwidth.

17. Traffic Management tools should not be used for anti-competitive purposes by preventing consumers from going to certain websites and applications. Strict adherence to net neutrality rules will prevent TSPs from dealing with traffic congestion in an appropriate fashion, so that service quality does not deteriorate.

18. Challenging situations that cause QoS to degrade can be summarized as follow :

18.1 Congestion, which caused by traffic overflow.

18.2 Delay caused by networking equipment low performance in large loads, as well as caused by distance or retransmission of lost packets.

18.3 Shared communication channels, where collision and large delays become common.

18.4 Limited bandwidth network with poor capacity management.

19. Service providers needs to show a technically justified rational for how they manage traffic, rather than for purely business reasons.

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

The management of the internet encompasses both technical and public policy issues and relevant intergovernmental organizations.

The Internet Governance principles that emerge for India should synergize the Indian democratic ethos and openness with the internet characteristic of the internet, namely, Openness, Dynamism, and Innovation.

There is a scope for India to consider and move towards governance mechanisms that are more open and participative and aim to see how it could influence Internet Governance domestically, regionally and Internationally to take into account concerns of emerging economies.

The borderless and distributed architecture of the Internet substantially differentiates Internet governance from traditional governance, challenging the established dominant role of nation-

states in policy making, access, human rights, privacy and standards have become important internet Governance issues.

Studies of Internet Governance have identified a lacuna in the field in that, many areas such as, Telecommunication policy, Information security, economics and cyber law that encompass aspects of Internet Governance, do not label themselves as studies of Internet Governance.

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.

1. The security and integrity of communications networks is of immense importance to the nation's economic infrastructure, strategic interests and social order. Therefore, the security of networks cannot be allowed to be compromised in any manner. Law enforcement agencies and national security agencies need to be provided access to communications networks and data regarding communications flow to protect larger public interest.
2. The providers of application services use advanced encryption technologies that impedes law enforcement agencies in lawful interception and monitoring. Such application providers are also not amenable to national legal jurisdictions. This has thrown

up new challenges for law enforcement agencies and Governments.

3. Due to global nature of the Internet, National security issues are not limited to domestic boundaries but have important international implications. Currently in the context of International Internet security there are no formally agreed upon definitions or treaties and there is little chance of applying traditional arms control regime to internet space.

4. *Develop human capacity for understanding the legal and technological issues related to internet security. This should be done for executives in the government departments. These should be joint sessions so that the participants get a holistic perspective. At another level, government could support launch of relevant courses in technological, management and law schools.*

5. The growth of OTT communication services has resulted in transfer of personal information, which poses a threat to national security and individual privacy. This calls for a need to examine the legal and regulatory framework.

6. Open architecture of the internet is responsible for the phenomenon growth of OTT services, it also causes the transfer of personal information on the internet to be fraught with potential risk and scope for misuse. OTT players are not regulated currently, so there are chances of abuse of this data.

The rapid proliferation of the OTT applications also are collecting large amount of private data of consumer, which needs to be protected.

7. OTT content providers should have to follow similar security and privacy rules which govern carriers besides having to adhere to licensing and revenue sharing conditions.
8. After Snowden revelations, there has been a renewed recognition in several parts of the world to review Internet Governance structure and those aspects that deal with sovereignty, surveillance, Cyber Security. Internet Governance issues are increasingly a proxy for a broader political struggle and for control of content.
9. Encrypted traffic is on the rise and it has implications for current differentiation techniques. In response to this increase, some satellite and in-flight network operators have deployed differentiation mechanisms that downgrade security properties of some connections to accomplish differentiation. The resulting risks to the security and privacy of end users can be significant.
10. Network operators should not downgrade, interfere with, or block user selected security in order to apply differentiated treatment. Network operators should refrain from preventing users from applying over the-top encryption or other security mechanisms without user knowledge and consent. Networks should not interfere with, modify, or drop security parameters

requested by an endpoint to apply differentiated treatment. Given the potential for possible exposure of sensitive, confidential, and proprietary information, prior notice should be given to end users of traffic differentiation features that affect security properties transmitted by endpoints.

11. Many countries such as Brazil have introduced data localization requirements to deal with security and surveillance threats. Notably, Blackberry was singled out in 2012 to install servers in India and to enable data decryption. Further, despite a policy directive for use of NIC emails for official purposes, many government officials send/receive formal emails from their Google, Yahoo or similar email applications.
12. TRAI *and DoT should actively monitor and enforce the use of NIC emails for official government communications.*
13. *It is recommended that since most of the data centers reside in the United States and Europe, efforts need to be taken to harmonize privacy regulations with these two jurisdictions.*
14. There should be various policies to create a framework for governance of the Internet and communications like :

- National cyber security
- E – mail
- National open data

15. Maintain the Security and integrity of network – Internet traffic also consists of undesirable elements like viruses, worms, spam, DOS (Denial of Service) attack etc. Therefore, it becomes important to protect the network elements from such undesirable traffic. *Since this is a legitimate requirement for maintaining the health of the network, it is not considered as violation of Net Neutrality.*

16. The government needs to be extra cautious in framing guidelines taking into consideration December 2015 incident in United States involving a terrorist's I-phone. Apple had declined to assist, saying that to do so would compromise the security of all I Phone users. The company argued that law enforcement officials didn't understand the consequences of creating a backdoor into the phone. The government would do good to address these concerns as well.

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

1. *It is recommended that the Intermediary Guideline Rules 2011 be reviewed and revised by way of in-depth open stakeholder consultations. The Intermediary Liability regime should be liberal such that it encourages service providers to host data domestically in India.*

2. *Intermediary Liability*: Intermediary liability is presently governed by Section 79 of the Information Technology Act73. A notice-and-takedown regime has been created for limitation of intermediary liability. The Section and its Rules there under have been under considerable challenge, including writ petitions before the Supreme Court of India, for having a chilling effect on free expression.
3. There is a need to examine the legal and regulatory frame work required for governing the privacy of users of OTT services.

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

1. There is also a need to regulate certain websites in India that feature objectionable content such as child pornographic. The TRAI and the Government has to find ways to manage online traffic and transparency in such a way so as keep the freedom of Internet Intact.
2. Carefully tailored rules need a strong legal foundation to service and thrive.
3. There should be detailed explanation of how and why these rules are to prevent challenge in the court.

4. There is a strong need for technology innovation from the service providers to reduce network cost and better utilize spectrum.
5. Some aspects like cyber security, Quality of service must be consider.
6. Indian ISPs want to be "Smart " when they went to discriminate with respect to content provided by OTT players but want to remain " Dumb " when they are accused of infringing copy rights due to nature of content transmitted by same OTT players.
7. Some applications, such as VoIP, could become unaffordable or could even be banned for many people, thus reducing their voice call options.
8. Higher flat rates would push up internet access costs for business and customers alike, and could result in a decrease in demand for online services because of their increased expense. This could have especially serious effects on businesses such as websites, selling high definition video downloads etc..
10. TRAI should regulate broadband rates or require providers to get permission to offer new rate plans or new services.

THANKS