CONSUMER PROTECTION ASSOCIATION

HIMMATNAGAR

DIST. : SABARKANTHA

GUJARAT

Comments on Consultation Paper

on

Net Neutrality

Introduction :

The development of the Internet relied critically on establishing an open process. Fundamentally, the Internet is a 'network of networks' whose protocols are designed to allow networks to interoperate. In the beginning, these networks represented different academic, government, and research communities whose members needed to cooperate to develop common standards and manage joint resources. Later, as the Internet was commercialized, vendors and operators

joined the open protocol development process and helped unleash the unprecedented era of growth and innovation.

Some traffic management practices can, on the contrary, prevent or limit innovation or freedom of expression, and even stem from discrimination, notably when the aim is to penalize or block competing content (in the case of an integrated supplier which is both a network operator and a content provider). As such, the ability to differentiate between types of traffic through the use of recent technologies is indeed raising concerns, and may justify placing limitations on their use.

We should restrict our attention to traffic management policies a subset of a larger class of network management policies. We should consider traffic management to mitigate the effect of congestion to address QoS, to address unwanted traffic or to address traffic potential harmful to the consumer.

To build the framework, we should focus both on the technical aspects of traffic management techniques and on the goals and practices of an ISP that uses these techniques.

The regulator's action with regard to Net Neutrality should be rely on several ongoing mechanisms that allow the authority to maintain a good understanding of the market, and to anticipate possible future challenges to the principles of Net Neutrality. These include regular score card on the quality of

services, thrice yearly information gathering, supervision of traffic management practice which include traffic management investigation report etc..

U.K. adopted a voluntary code of practice, where as the Netherlands and Slovenia choose instead to adopt dedicated law to protect Net Neutrality, explicitly prohibiting ISPs from engaging in certain practices.

The European regulation introduces a strong principle: Providers of internet services shall treat all traffic equally, without discrimination, regardless of the sender and receiver, the content, or the terminal equipment used.

Q.1 How should \Internet traffic" and providers of \Internet services" be under stood 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?

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

Please provide reasons.

Comments :

Internet Service providers :

* An Internet service provider (ISP) is an organization that provides services for accessing and using the Internet. Internet service providers may be organized in various forms, such as Commercial, Community owned, non profit or otherwise privately owned.

  ISPs do not operate the Internet, instead they sell access to the Internet to their customers, often bundled together with a range of other services, such as, Web-based e-mail, Telephone (Conventional or VoIP), Cable Television and so on. They sit, in other words, near the edges of the Internet, providing a Link between the end users and the Internet.

* Is a company that provides retail access to the internet for members of the public or for businesses and other organizations those connections may be via cable, DSL, Satellite, wireless, Dial up or any other Technologies.

* An Internet Service Provider (ISP) is a company who provides third parties access of the Internet.

* An ISP who has the equipment and the Telecommunication line access required to have a point - of – presence on the Internet for the geographic area served.

* An ISP who acts as an Intermediary between its client's computer system and the Internet.

* ISP who take several forms and offer a wide variety of services.

* ISP who generally charge their customers for Internet access depending on their usage needs and the level of service provided.

* Who provides the large computing systems and data storage required for other users to connect to the network of computer/mobile connected by a common protocol.

* Is an entity that provides its customers the ability to obtain online information through the internet.

Internet Traffic :

Internet traffic is the flow of data moving across the Internet network at a given point of time. Network data is mostly encapsulated in network packets, which provide the load in the network. Network traffic is the main component for network traffic measurement, network traffic control and simulation.

Internet traffic is also known as Network traffic or data traffic.

Internet of Things (IoT) :

There are both positives and negatives emerging in the IoT space as a result of Net Neutrality. There will be things like simplified service deployment, growth in deployment of BYO – type application, a drop in carriage costs-especially for high – bandwidth needs to lower levels without bias, and can also avoid " premium content " providers jeopardizing service quality level.

On the negative side, there are two main concerns. First net neutrality will prevent valid opportunities to use next-gen networks for critical services that validly would have priority route management (e.g. first responder, medical alert

etc.). This will continue to foster proprietary network build and need. Second, it will prevent the development of valid, " multi – tier " commercial pricing models, where best efforts at a low price may be attractive.

These two things should be considered.

However, as more and more IoT applications emerge, some provisions can be needed to be applied and probably tested to determine what might be considered " fair and reasonable " within the context of IoT.

The meaning of " unjust and unreasonable discrimination " should be fully played out within the contact of IoT . It seems reasonable to assign priority access, to some applications, e.g. sensitive Health Monitoring applications or Public safety applications, but until those provisions have some IoT relevant parameters, this will be an area of uncertainty.

Q.2 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).

Comment :

The broad approach.

We should not adopt the " Narrowly or carefully tailored " standards. Because, this standard is unnecessary restrictive and may overly constrain network engineering decision. More over " Narrowly tailored " language could be read to import strict scrutiny doctrine from constitutional law, which are not persuaded would be helpful hear.

Reasonable traffic management by ISPs, should be acceptable in only limited circumstances, and must not be based on commercial consideration.

ISPs should be prohibited from degrading or blocking traffic (or certain categories of traffic), except under clearly defined circumstances. These practices are justifiable in only a small number of instances :

1. To comply court order
2. To protect the integrity or security of the network.
3. To protect the integrity or security of the Nation
4. To prevent impending network congestion, that occurs temporarily, unforeseeable cases of network congestion and under exceptional circumstances.

Q.3 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 users choice and without any arrangement between a TSP and content provider, be treated?

Comments :

We should restrict our attention to traffic management policies as a subject of a larger class of network management policies. We should consider traffic management to mitigate the effect of congestion to address QoS, to address unwanted traffic or to address traffic potentially harmful to user.

(a) What should be regarded as reasonable TMPs?

Regulation in Canada, The United States and other jurisdictions have generally accepted the notion of " Reasonable network management " as a part of Network Neutrality. In Indian contact it will also be useful.

Network Management " Reasonability :

1. The service provider should not prevent any of its users from sending or receiving the lawful content of the user's choice over the internet.

2. The service provider should not prevent any of its users from running the lawful applications or using the lawful services of the user's choice.

3. Service provider should not prevent any of its users from connecting to and using on its network the user's choice of lawful devices that do not harm the network.

4. The service provider should not deprive any of its user's entitlement to competition among Network providers, Application providers, Service providers and Content providers.

5. The service provider must treat lawful content, Applications and Services in a nondiscriminatory manner.

6. The service provider must disclose such information concerning network management and other practices as is reasonably required for users and content, Application and Service provider to enjoy the protection specified in this part.

Reasonable Network management consists of :

Reasonable practices employed by the service provider :

1. (i) Reduce or mitigate the effects of congestion on its network or to address quality of service concerns.

   (ii) Address traffic that is unwanted by users or harmful.

   (iii) Prevent the transfer of unlawful content, or

   (iv) Prevent the unlawful transfer of content

2. Other reasonable Network management practice.

The regulation should describe three specific exceptions which are allowed under stricter conditions. These are :

1. Compliance with other Law.

2. Preservation of integrity and security and

3. Congestion management measures.

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

To be successful, reasonable network management to address problems such as Congestion must aim for precision and success in terms of a desired technical effect. It must do so by enhancing Subscriber Quality of Experience (QoE) to stay ahead of competitive forces, and also without falling afoul of public perception and official regulation. Success adhere to the following best practices :

1. Legitimate and demonstrable Technical need :

The operator must have a legitimate and demonstrable technical need for the network management practice. The architectural strengths and weaknesses of various network access types provide the majority of the technical needs for network management.

A network management practice that is unreasonable in one access network may well be reasonable in another. This context is crucial. Solutions fair best when they directly address the problem of a legitimate network problem such as congestion and do so with proportional precision.

To be successful, a traffic management practice must be described in such a way that both the technical need and the practice are clear and the traffic management practice seeks only to address this need and nothing more.

2. Narrow – Tailoring in terms of the stated technical goal of a traffic management practice :

All networks have variations in usage patterns, whether by time of day, by geography, by user demographics or other factors. As a consequence, oversubscription and QoE are non-uniform across the network. A properly constructed network management plan takes this into account, and focuses as narrowly as possible on the problem to be solved. It does not try to force a one-size-fits-all solution into all areas at all times. When applied correctly, management of traffic during times of congestion is a win-win as the majority of subscribers continue to have a good QoE and the access network lifetime is extended, allowing network investments to made in other areas of need. In an access network environment, there are several areas of 'narrowly-tailored' that might be technically considered for addressing subscribers who are causing disproportionate congestion. These include:

- Network type
- How access nodes and links interact
- Subscriber density per access node
- Subscriber demographics per access node
- Backhaul network capacity
- Unforeseeable events

A reasonable network management practice takes these factors, and more, into account. It applies itself differently, or not at all, depending on the conditions

that are currently present. For example, a network management practice might be self-tuning, and could disable management when no congestion is present. In a cable network it might operate differently when congestion is present on a single user, versus on a single RF channel, versus on a bonded set of RF channels, versus on the CMTS backhaul uplink. It might detect congestion passively by setting a maximum bandwidth threshold per node and monitoring the bandwidth usage, or it might do so actively by measuring the real-time latency in the access network and triggering according to a latency threshold attached to subscriber quality of experience. A successful traffic management practice will narrowly-tailor itself to the situation at hand at the time it is needed. It will not apply in a broad fashion across the broad average of a network.

3. Proportional and reasonable effect in achieving the Goal :

The network management policy needs to take into account the concept of proportional effect and response. A 'reasonableness' test helps define the acceptability of network management. This test stems from the common-law concept of 'what would a typical person agree is reasonable', and is therefore somewhat subjective in definition. Some precision of what is reasonable can be achieved through the best practice of seeking proportionality in term so the final outcome of a policy seeking to address a problem such as network congestion. It has been proven that long-term heavy users are not the contributors to congestion when it occurs, which makes targeting long-term heavy users during times of congestion out of proportion, inaccurate, and therefore not reasonable. Similarly, it would be considered unreasonable by most to take a subscriber causing 15% of the congestion on a network and manage their bandwidth to 1%

of peak rate for all time. However, a reasonable argument for fair distribution can be made to reduce the priority of traffic of the top twenty-percentile of bandwidth users during times of congestion, which as a group typically constitute only 5% of subscribers but consume more than half the network's bandwidth at a given point in time. In reducing the traffic priority of this ever-changing minority during times of congestion the latency, and by extension QoE, of the other 95% remains good. Reasonableness can be defined through contract, which means it relates directly to the best practice of transparent disclosure described below. If typical users, understanding the disclosed network management policies in use, contract for the service, the policy must be reasonable by definition. Reasonable is defined entirely in the frame of reference of the end-user, the customer of the service provider.

4. Transparent Disclosure :

Transparency is a challenging concept. The subtle technical nuances of networks (latency, loss, jitter, shared-access, etc.) are difficult to describe in simple enough terms for the average layperson. Analogies, although helpful to form a basis, rapidly become inappropriate as they diverge from the original problem. Network management practices evolve over time, and new technologies have seen the emergence of traffic management practices based on deep packet inspection (DPI). Since we are relying on transparency as a means of supporting reasonableness, what's relevant to disclose is any aspect that would affect the actions or perceptions of the typical consumer. The operator must make the material information publicly available to allow understanding of the network management policy by those impacted by it. The disclosure should be sufficient

for a consumer to form an informed opinion on whether the practice will affect them, which applications might be affected, when they might be affected, and what the impact might be, including impact to speed, latency and general experience. Similarly, subscribers should be notified in advance of any planned changes to network management practices. Disclosure might take many concurrent forms. The most popular include network management FAQs, notices included in billing material, acceptable use policies, terms of service, etc.

Service providers are subject to strengthened transparency obligations. These pertain in particular to providing more detailed information in consumers contracts : the possible impact of traffic management techniques used by the ISPs, concrete impact of the (traffic, speed etc.) caps or allowances attached to the plan, information on connection speeds, etc..

5. Auditable and Demonstrable :

Owing to the public scrutiny of capital investment in networks, and network management policies, it becomes important for a ISP to demonstrate that the above criteria were indeed met. On audit, a service provider should be able to provide the following:

1. Justification of the technical need that caused the creation of the network management policy.
2. What affect the policy had on the user experience.
3. How they have disclosed their policy to the end-user.

4. How the policy took into account network and time variances (i.e., how it was tailored).

In addition, the audit should be able to demonstrate the above were met using technical results. These results might include information on the user experience for the typical user for typical locations in the network.

In short Network management policies based on traffic management must be technically legitimate, narrowly tailored, proportional and reasonable, transparently disclosed and auditable. Reasonable network management requires disclosure of the policy in such a way that the typical user can understand the impact to them, and reasonableness is framed entirely from the end-user perspective. Access-agnostic network policy control is required to create a network management practice that spans multiple devices, and multiple access technologies. The network management practice must take into account the specific conditions of the access technology. Strong reporting and business intelligence is required to be coupled to the network management practice to support auditing and the understanding of demand, capacity, and user experience. As a typical service provider, this may seem like a minefield of requirements, but a few simple up front planning activities can make for a highly successful traffic management practice.

A framework for determination of whether a traffic management practice is reasonable :

The location in the network where the traffic management technique is applied is most important. If the technique is *applied at an endpoint*, it should be classified as a reasonable traffic management practice regardless considering other things. One endpoint is the user; practices applied directly by the user are not in question. The other endpoint is the entity with

which the user is communicating. When this entity is an ISP, the ISP is acting in the role of an application provider. Common examples of this situation are ISPs that offer email and/or web hosting services. However, a user can (or should be able to) receive such application services from a large number of potential providers. Since this market is competitive, practices applied at an endpoint that negatively impact the user's experience may drive users to change application providers, buy they need not change their ISP. Therefore, any traffic management practice applied at an endpoint should be classified as reasonable. In contrast, if the traffic management practice is applied *at a transit node*, we must consider the other things.

Next consider the \who" question, namely who decides whether the traffic Management practice is applied. If, traffic management practice is applied directly by a user or by an ISP only when a user desires this action, it should be classified as a reasonable traffic management practice because the user has control over whether the practice is applied. Such practices are common, and include many firewalls, parental control software, and tiring. If an ISP were to provide enhanced QoS for voice or video purely on the basis of consumer payment, then this payment for QoS would not be discriminatory and it be classified as a reasonable traffic management practice. In contrast, if the traffic management practice is an action taken unilaterally by an ISP, then it is worthy of further investigation. If a practice is used without user consent, then we believe it should be disclosed in sufficient detail in the user contract. If so disclosed, then we must consider the remaining questions to determine if it is a reasonable practice.

we only consider lawful and non-harmful uses of the network; security measures may require special considerations. We do not consider issues of privacy, which intersect with many of the techniques discussed here but which require considerations beyond those detailed here. **Prohibition of unreasonable practices should implemented where sufficient competition does not exist.**

The next aspect to be considered is the \what" question, in particular whether

the practice involves blocking or termination of a session versus enhancement or degradation of QoS. If the practice involves *blocking or termination*, we propose to classify it as unreasonable. Blocking or termination practices that are applied at a transit node without user choice are unreasonably anticompetitive, cause undue harm to consumers, or unreasonably impair free speech. When blocking is applied at a transit node without user choice *on the basis of the source or destination or on the basis of the speech within the packet*, the practice unreasonably impairs free speech; this type of blocking includes blocking of specific web pages or blocking on the basis of the content

of the speech. When blocking is applied at a transit node without user choice *on the basis of the application*, the practice is unreasonably anti-competitive and/or causes undue harm to consumers; this type of blocking includes blocking of specific applications (e.g. blocking or terminating VoIP or file-sharing connections) and blocking of specific ports (e.g. SMTP or server ports). There is no reasonable justification for the use of these techniques. In some cases, the ISP's goal may be to limit congestion, reduce spam, or implement security; however, such goals can be implemented either through less severe methods that do not involve blocking or with the consent of the user. If a traffic management practice is implemented in a transit node, without user choice, but does not block or terminate connections, we must consider the remaining questions. Practices that *enhance or degrade QoS in a transit node without user choice*

are the concern of the remainder of this section of the paper. To address such practices, consider the \when" question, which asks on what basis is it decided to apply the traffic management practice. This question considers the manner and purpose of the practice. We propose that the pertinent distinction should be whether the traffic management practice is applied to certain traffic on the basis of (i) the application, (ii) the source and/or destination, (iii) service provider, and/or (iv) payment.

First, consider using *source and/or destination and/or service provider* as the basis. A common example of this practice is an ISP that provides enhanced QoS for its own VoIP service, but does not provide this same QoS to competitors VoIP packets. Another example of an exclusive arrangement would occur if an ISP were to provide access to enhanced or degraded

QoS to some third party application providers but not others. Use of source and/or destination and/or service provider without user choice involves the use of exclusivity. Such exclusive arrangements are unreasonable, since they tilt the playing field between application providers through use of Internet infrastructure. Thus, these traffic management practices be classified as unreasonable,

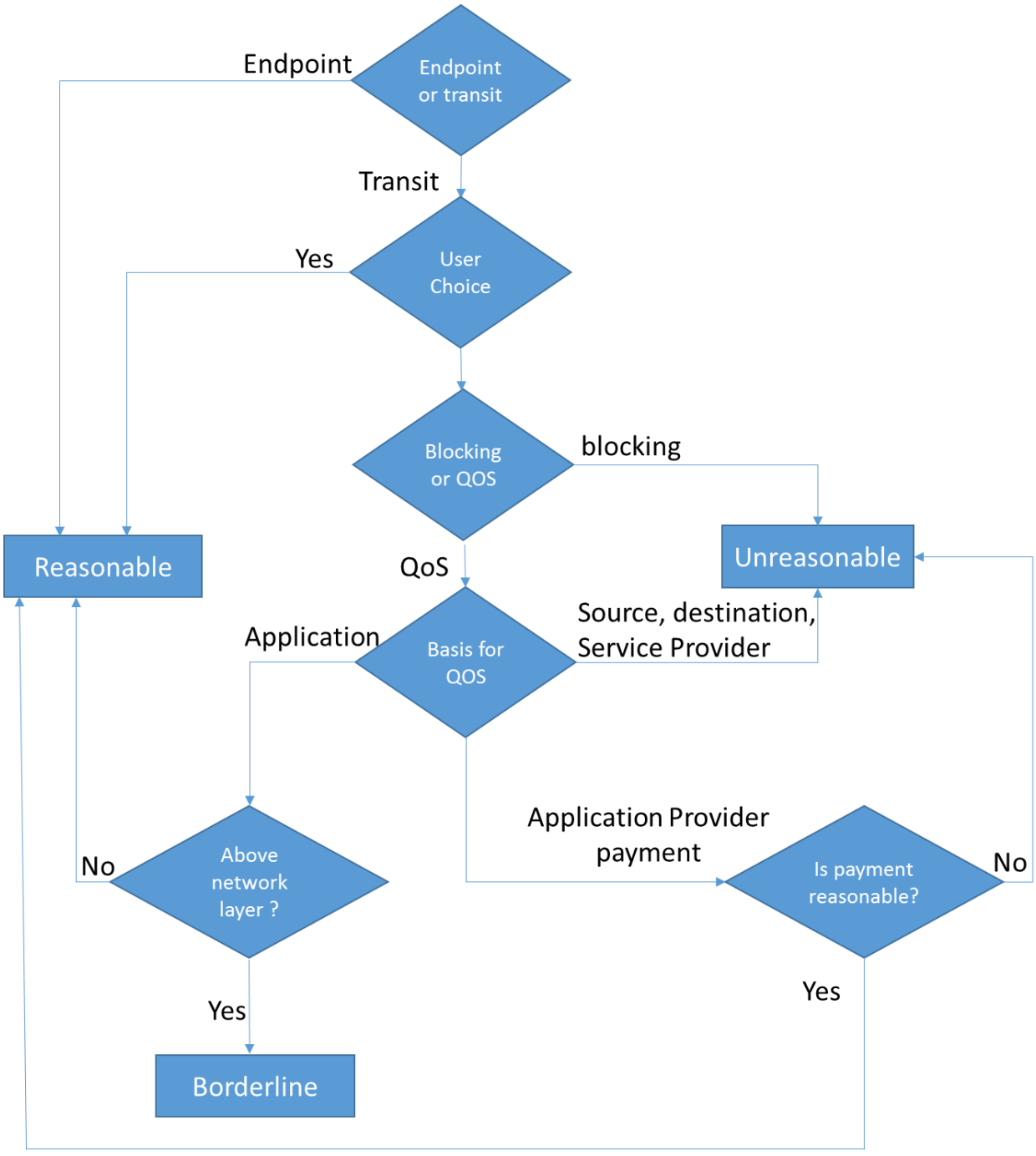
because they are unreasonably anti-competitive.

Next, consider using *payment* as the basis for the decision of when an ISP uses enhanced or degraded QoS. If the price is not unreasonably discriminatory (e.g. if an ISP sells QoS to all application providers at the same price as it passes on to its own applications that require QoS), then the practice is reasonable. However, if prices for QoS are unreasonably discriminatory, then a traffic management practice that uses such prices as the basis is unreasonable since the practice is unreasonably anti-competitive.

Finally, consider cases in which the practice is applied on the basis of the *application*. In these cases, if the practice is applied entirely *at or below the network layer*, then the practice be classified as reasonable. Enhancement or degradation of QoS is thus applied to specific packets identified by the user, for instance if an ISP chose to give enhanced QoS to all packets identified using diffServ code points by the user as VoIP.

The last remaining case consists of practices that are applied *at or above the transport layer at transit nodes without user consent and enhance or degrade QoS on the basis of the application*. Practices of this sort use DPI to identify which packets should receive high or low priority or dedicated bandwidth. A common example of this practice is traffic shaping for file-sharing. Because DPI is used (rather than user identification of these packets), this practice violates layering. The question is whether this violation of layering is severe enough to cause this practice to be classified as unreasonable. There are more direct techniques that can be used that rely on user identification of packet priorities and that do not violate layering. However, because these alternative practices involve different business models that may require some time to be accepted by the public, we recommend classifying any such practice that uses DPI to apply QoS as a borderline traffic management practice that could be used for a limited period of time if properly disclosed in the user contract.

The resulting framework is summarized in following figure :



Q.5 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.

Comments :

Yes.

* Practices that block or degrade the transmission of the service , or a type of service, only under these defined circumstances .

Other services :

1. To Comply with a legal decision or court order.

2. To mitigate temporary and exceptional network congestion.

TRAI should supervise these practices, inventorying them and accessing impact on the quality of internet access services.

Q.6 What could be the principles for ensuring nondiscriminatory access to content on the Internet, in the Indian context?

Comments :

General Principles :

1. **No Blocking**: broadband providers should not block access to legal content, applications, services, or non-harmful devices.
   - **No Throttling**: broadband providers should not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non- harmful devices.
   - **No Paid Prioritization**: broadband providers should not favor some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind—in other words, no "fast lanes." This rule also bans ISPs from prioritizing content and services of their affiliates.

2. ISPs should not " unreasonably interfere with or unreasonably disadvantage " the ability of consumers to select, access, and use the lawful content, applications, services, or devices of their choosing; or of edge providers to make lawful content, applications, services, or devices available to consumers.

3. The rules should be apply equally to broad band services provided via fixed or mobile wireless platforms equally to all ISPs, regardless of technology used.

4. The ISPs should make publically available the terms and conditions of their services offering.

5. Broadband ISPs should disclose, in a consistent format, promotional rates, fees and surcharges, and data caps. These disclosers must also include packet loss as a measure of network performance and provide notice of network management practices that can affect services to the authority.

Smaller broadband ISPs can be given temporary expansion from these requirements. The authority can maintain or revise that expansion.

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?);

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

Comments :

Mentioned above.

Q.8 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.

Comments :

In the United States User's ability to attach devices of their choice to the telephone network is guaranteed by regulation, providing that the device does not harm the network. The federal Communication Commission (FCC) has also created a regulation that gives users the right to use non harmful devices of their choice on fixed internet broadband.

We believe a balanced approach that provides rights to both stakeholder groups will maximize social welfare. Following consumer rights should be prevented :

1. Consumer should be entitled to connect any legal device to a communication network, so long as device does not cause harm to the network.

Definition of Harm :

The term harm means electrical hazards to the personnel of providers of communications, damage to the equipment of providers of communication, malfunction of the billing equipment of providers of communications and unreasonable degradation of service to persons other than the user of the subject terminal equipment, his calling or called party, unreasonable degradation includes harmful interference, defined as any emission, radiation or induction that seriously degrades, obstructs, or repeatedly interrupts a communication service. The term unreasonable degradation can and should be interpreted to include security problem.

2. Consumer should be entitled to run applications of their choice on their devices.
3. Consumer should be entitled to choose a communication provider in a competitive market place.
4. Consumer should be entitled to transparency in terms of billing, tariff management, device restriction and all other aspects of their communication services.

Smart phone used on cellular network are in greater challenge to open networks. A cellular provider often exercises control over the devices used on its network through a combination of terms of service and device pricing. The provider often reserves the right to control nearly all communication protocol over the device. It is not uncommon for providers to lock devices to their own networks or to cripple functionality of devices.

User ability to connect devices of their choice, standardized protocols, and shared control based on effectiveness are violated by many devices offered by or mandated by ISPs. Such restrictions impede the development of a competitive heterogeneous market for devices.

A great need exists to create a unified legal frame work that can dictate a user's right to attach devices to future telephone and cellular internet network.

Industry or TRAI should define a basic air interface for wireless devices, and that this basic air interface be used to prohibit cellular carriers from banning attachment of any compatible non-harmful device.

Q.9 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;

(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?

Comments :

A combination of the above.

Regulatory control required.

Q.10 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.

Comments :

Agree with the Template at Table 5.1

It should be easily understandable for the consumer.

Q.11 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?

Comments :

There should be a multi – stakeholder consist of representation from TSPs, Consumer groups registered with TRAI, Content providers, Civil society, Academic/Research organizations, Technical and operational experts etc. to monitor and comply NN rules under the guidance and supervision of TRAI.

TRAI has sufficient powers to handle NN. If needed should be empowered. Systematically indulging discriminatory practices should be dealt by TRAI and appropriate regulatory intervention, along with strict penalties and other legal actions should be immediately taken by the authority.

Levying heavy penalties for NN violation is the important tools. The penalties must be " effective, proportionate and dissuasive ", issuing cease and desist orders in case of infringement, combined with periodical penalties or fines.

Q.12 What could be the challenges in monitoring for violations of any NN frame-

work? 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 (re-search studies, news articles, consumer advocacy reports).

Comments :

Combination of all three. Discussed above.

Q.13 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?

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

Comments :

We support self regulation in which all licensed providers or Internet services to follow a voluntary mechanism for adhering to core principles of NN as identified through the process, with a self regulatory monitoring mechanism that would function under the overall guidance of the Authority. For this purpose

Annual meetings with Stake holders and CAGs should be organized to monitor the status of NN.

Q.14 What mechanisms could be deployed so that the NN policy/regulatory framework may be updated on account of evolution of technology and use cases?

Comments :

Proactive close monitoring and compliance should be done by TRAI with Annual evaluation meeting with Stake holders and CAGs. Research in this area should be carried out by the authority.

* In Many countries internet service providers are legally required to allow law enforcement agencies to monitor some or all of the information transmitted by the ISP. Further, in some countries ISPs are subject to monitoring by Intelligences. (Note : Potential violation of the privacy protection should strictly be prohibited)

* Modern ISPs integrate a wide array of surveillance and packet sniffing equipment into their network, which then feeds the data to Law-enforcement/Intelligence networks allowing monitoring Internet traffic in real time.

(Dr. Kashyapnath)