Pre-Consultation on Net Neutrality

Dear Sir,

We welcome the opportunity to submit our views on the Pre-Consultation paper on Net Neutrality, dated 30th May, 2016, by Telecom Regulatory Authority of India (TRAI). We are providing a general response to the topic raised in the Pre-Consultation paper following by a detailed response to each of the questions.

Regards,

Authors[1]:

- Prof Rekha Jain, Executive Chair, IITCOE, IIM Ahmedabad
- Mr Amod Prakash Singh, Researcher, IITCOE, IIM Ahmedabad
- Mr Rishabh Dara, Student, IIM Ahmedabad

[1] All views expressed are personal. The authors acknowledge the contributions made by Ms Radha Ravattu (IITCOE) and Mr Pranesh Prakash (CIS Bangalore) in framing the comments previously submitted to TRAI in response to the Consultation Paper on Regulation of OTTs in 2015, on which the present submission is based.

Net Neutrality

Net Neutrality is not a singular construct. Thus one is neither simply for or against net neutrality. Net neutrality needs to be broken down into its various components and exceptions; and then contextualised to the unique features of the Indian policy environment.

Over time, net neutrality has become a political issue wherein individuals or groups have taken a for-or-against stance. Keeping that in mind, TRAI must, in essence, endorse the overall concept of net neutrality and the open nature of the internet. Any contrary decision could send a wrong signal to activists, investors and friendly countries. Nevertheless, while endorsing net neutrality and an open Internet, TRAI must not treat net neutrality as a non-violable religion. TRAI must simultaneously recognise that net neutrality, as a policy construct, is not well defined and has different interpretations in different contexts. Specifically, in India, the interpretation of "net neutrality" is definitely a function of the Indian context. It is coloured by the evolving nature of technology, networks and markets.

Uniqueness of Indian Context:
Contextualizing Net Neutrality to India, one needs to understand that it is a one-of-its-kind market with unique characteristics. Such as:

1. Dependence on wireless internet access (in contrast to wireline broadband)
2. Limited, fragmented and non-contiguous spectrum available with Indian TEL-SPs
3. Low spectrum/population
4. High cost of spectrum (price per MHz. per capita)
5. Low broadband penetration; Low penetration of 3G and 4G services
6. Lack of content in vernacular languages
7. Most content is hosted outside the country; most data is routed outside the country
8. Low enforcement of IT Act with foreign intermediaries
9. National security concerns are higher in India than most other countries
10. High competition between TEL-SPs; relatively low switching costs
11. Perceived relevance of Internet to a large number of people
12. Low levels of digital literacy
13. Perceived equivalence of Internet and Facebook+Whatsapp
14. High sharing of passive and active infrastructure

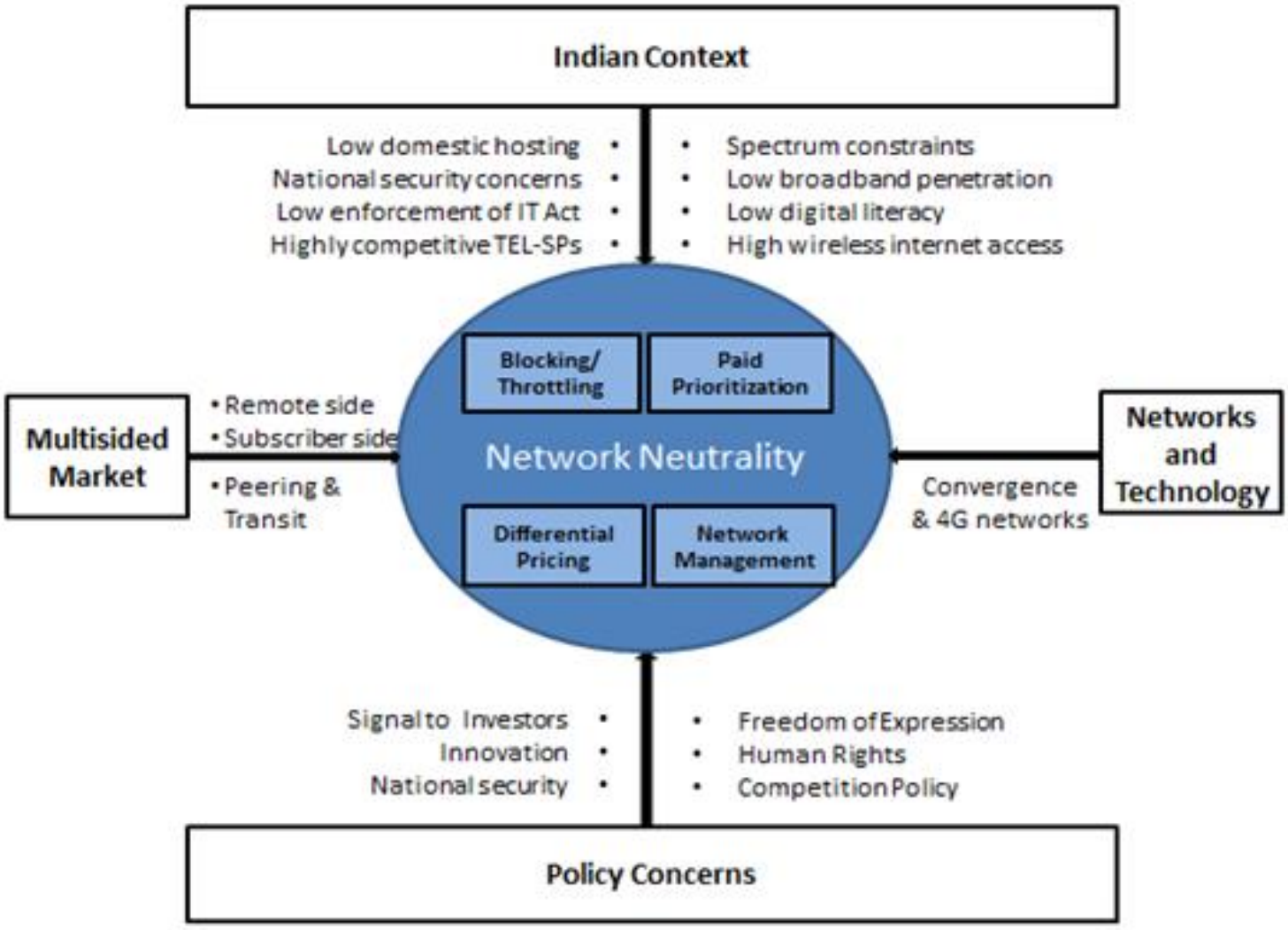
Evolving nature of Technology, Networks and Markets*:*
Technology, networks and markets are constantly evolving at a very fast rate. We capture a few important aspects that TRAI should keep in mind while developing its recommendations:

1. *Convergence and 4G Networks*: With the advent of 4G, networks have transitioned from circuit switched networks to fully packet based networks. Like Internet Based Services (e.g. Skype calls), now traditional services (e.g. PSTN voice calling) are also capable of being delivered over an IP based network and may share the same infrastructure as Internet based services. India has also moved forward to the Unified Licensing regime in which, the Unified License (with authorisation for Access Services) now allows for interconnection between IP Telephony and the PTSN/PLMN network.

2. *Evolving Nature of Market & Network*: The historical assumption of a TEL-SP only having a relationship with the local subscriber and peering/interconnecting networks is no longer true. Over time, the market for a last-mile network has evolved into a multi-sided market. Besides the "local" side of delivery of internet access services to the subscriber, the TEL-SP also shares a "remote" side with OTT-SPs that are not directly

interconnected with the last-mile network. Increasingly, many content providers are now also directly interconnect with last-mile networks through content delivery networks. This evolving nature of the network architecture and market needs to be accounted for in the contextualisation of constructs and issues.

The following diagram captures the essence of the submissions above and provides a framework for Net Neutrality.



Questions:

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?**

In our submission, we recognize the following components and exceptions of net neutrality

- No Blocking
- No Throttling
- No Paid Prioritization.
- No Differential Charging
- Transparency
- Reasonable Network Management
- Specialized Services

For each of the components and exceptions, the response is structured as:

1. Views for.
2. Views against.
3. International practices.
4. Recommended principles.

No Blocking:

Views For:

- The concept of open internet is essentially based on the idea that no lawful content or non-harmful device can be blocked from the Internet.
- Freedom of Expression Issue: TEL-SPs should not wear the hat of the judiciary and be able to decide which content, application or service should be available to the end user.
- TEL-SPs may misuse the threat of blocking to extract differential income from different OTT-SPs.
- TEL-SPs may block certain services to influence competition and promote their own services.

Views Against:

- A lot of unlawful content is publicly available on the internet.
- People may want specific categories to be blocked. For example, the user doesn't want specific content to be accessible by their children - parental control services offered by TSPs.
- Harmful devices which have a negative impact on the security and stability of the network or end user can be easily used
- In the public WiFi networks where the network is shared by large number of people, the sites which consume higher bandwidth will decrease the quality of other services[1]

International Practices:

- The US Open Order 2015 states that no blocking is allowed. "A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management."[4]

Recommendations:

- TRAI should recommend to DoT that the terms and conditions of the Unified License agreement should be amended to enforce a no-blocking requirement for both incoming and outgoing traffic
- This should be subject to the exceptions identified under reasonable network management outlined later in the submission.
- In all other situations, blocking of content should only be possible under a direction under Section 69A or 79 of the Information Technology Act.
- Networks may block devices that do not comply with industry established standards if they have the potential to affect the security and stability of the network.

No Throttling:

Views For:

- Throttling is equivalent to blocking since the effective consumption of a service would be reduced if its quality of service is degraded.
- Throttling, if service specific, will allow the TEL-SP to charge OTT-SPs.

Views Against:

- Given spectrum constraints (limited, fragmented and non-contiguous), network management practices are extremely important in India.
- Not all data requires the same QoS. For example, real time services like voice/video call require higher priority than non-real time services like email wherein slight jitter is not an impediment. Effective network management may require throttling of non-real time services.
- Both IPv4 and IPv6 reserve space for DiffServ/ToS in the headers implying that the Internet was technically never conceived to treat all packets the same.
- Certain services like torrents for downloading movies consume a lot of network resources effectively degrading the quality of service for more essential services.

International Practices:

- The US Open Order states that No throttling is allowed. "A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management."[5]
- The US Open Order report of 2010 recognises that "in some circumstances the distinction between blocking and degrading (such as by delaying) traffic is merely semantic."
- The Netherlands law for net neutrality states that "Providers of public electronic communications networks over which Internet services are provided and providers of Internet access services hinder or delay any services or applications on the Internet"[6]

Recommendations:

- Rules for throttling should be similar to blocking.
- An exception for throttling may be created for real-time versus non real-time classes of services.
- Throttling should be allowed to deal with the situations identified in reasonable network management as identified later in the submission.

No Paid Prioritisation:

Views For:

- OTT-SPs with deep pockets will be able to enter into deals with TEL-SPs to prioritise their data. Smaller competing OTT-SPs will not be able to afford such prioritisation - thus affecting competition and innovation.
- It is a zero sum game in which prioritisation of some services may have a direct negative impact on other services when there is congestion.
- Paid priority agreements can be a threat to non-commercial end users, including individual bloggers, libraries, schools and advocacy organizations.
- Paid prioritization may be seen as giving TEL-SPs an incentive to limit the quality of service provided to non-prioritized traffic.

Views Against:

- There is a need for prioritisation of public services that require higher quality of service like emergency health services.
- These are free market deals and the regulator should not intervene.
- Both IPv4 and IPv6 reserve space for DiffServ/ToS in the headers implying that the Internet was technically never conceived to treat all packets the same.
- Users can anyway purchase packages for higher bandwidths, which as a result of the zero sum game, have a negative impact on other users.
- Certain services like real-time voice calling may require to be prioritised over other services to maintain quality of service.
- As an alternative to paid prioritisation, OTT-SPs with deep pockets can use CDNs with closer geographic location to get their data delivered faster to achieve higher quality of service. Therefore paid prioritisation will not have a significant impact on competition.

International practices:

- The US open order 2015 states that paid prioritisation should be banned. "A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not engage in paid prioritization."[7]
- Paid prioritization defined according to US open order "refers to the management of a broadband provider's network to directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either (a) in exchange for consideration (monetary or otherwise) from a third party, or (b) to benefit an affiliated entity."
- Under the Federal Communication Commission (FCC) order of March 2015, "Reasonable Network Management is an exception to the no-blocking rule, no-throttling rule, and no-unreasonable interference/disadvantage standard, *but not to the rule against paid prioritization*." "this Order contains an exception for reasonable network management, which applies to all but the paid prioritization rule (which, by definition, is not a means of managing a network):"

Recommendations:

- Paid prioritisation should not be allowed.
- Reasonable network management should not be allowed as an exception to paid prioritisation since it is not a form of managing a network.

- CDNs, paid peering, and other such arrangements should not be considered as prioritisation as they do not change the priority of the data packets.
- CDNs and other ASs should be allowed to directly interconnect with NIXI. Currently only licensed ISPs are allowed to interconnect with NIXI. NIXI should be restructured in terms of its composition, and its billing model should be changed to allow for settlement-free peering.[2]
- TRAI should forbid TSP from charging OTT-SPs a termination or content-carriage fee for terminating data on their network, or engaging in any degradation of any quality of service metric with an aim to charge for carriage of content or for creating incentives for paid prioritisation.

No Differential Charges:

Views For:

- If charges are set low for certain apps:
    - Walled Garden: People's conception of the internet may get restricted to a few services that are zero rated.
    - Competition: Given the free data access, users would prefer using zero rated services which may hamper competitiveness of startups that cannot afford zero rating deals.
    - Over-consumption: With zero rating and free usage of Internet there is a chance for wastage of network resources.
- If charges are set high for certain apps:
    - Charges may be set high for certain apps to extract income from them, thus creating an non-level playing field and hindering innovation.
    - Lack of predictability in OTT business model if charges are suddenly set high.
- General concerns:
    - Deep packet inspection to make app or content specific decisions may lead to privacy concerns.
    - If charges are set for a class of service (like VoIP calling), then those apps providing mixed services (like gaming with VoIP) may lead to difficulty in classification.

Views Against:

- If charges are set low for certain apps:
    - People from economically under-privileged backgrounds will be able to access services for free, which they may not be able to access otherwise.
    - Zero rating will help in the increase of Internet penetration especially in the emerging economies.
    - Zero rating of e-governance services should be permissible.
    - Zero rating can be used as an instrument for promoting proliferation of content in vernacular languages.
- General concerns:
    - Subscribers have differential preferences and may prefer to pay lower charges for a select bouquet of apps or services.
    - Different apps have a different impact on network congestion, thus imposing different costs on the network.
    - Different apps affect the business model of TEL-SPs differently. TEL-SPs should be able to charge OTT- SPs accordingly. For example, a VoIP calling facility will lead to substitution of traditional telecommunications services

[2] http://www.iitcoe.in/download.php?file=paper/97UnshacklingtheNIXI%20Legacy.pdf&hits=39&id=97

International Practices:

- Netherlands law states that "The level of tariffs set by the Internet access service providers for Internet services should not depend on the services and applications offered through it."[8]
- FCC doesn't treat all zero rating in the same way. Under the Federal Communication Commission (FCC) order of March 2015, the legality of zero rating falls within the legal grey area of the FCC's "general conduct" rule, which demands a case-by-case analysis to determine whether the conduct causes unreasonable discrimination or disadvantage, based on an array of factors including effects on end-user control, competition, consumer protection, innovation and free expression.

Recommendations:

- The TRAI may amend the Regulation on Differential Pricing and allow zero rating of e-governance initiatives.
- Over time, as data charges reduce and access to the Internet increases, zero rating will become redundant. The issue of zero rating is therefore transient. The TRAI may amend the Regulation on Differential Pricing and allow zero rating with a sunset clause for 5 years.
- FRAND & TSP Agnostic Regulations: It is recommended that zero rating be permissible if and only if it is done in a non-discriminatory and transparent manner, within a regulated marketplace, with specific anticipated anti-competitive practices being clearly prohibited ex-ante, and an easy to access and swift redressal mechanism for failure to abide by the regulatory framework. In this, the platform should be open to all internet based service providers without discrimination. The terms for using the platform (including prices) would be openly transparently published and uniformly applicable to all. The TRAI Consultation on Free Data partially addresses this issue.
- USOF and Digital India funds may be used for providing 200 MB unrestricted data packs to those persons that satisfy a prescribed criteria on the basis of geography and income; or for subsidising such initiatives by startups.

<u>Transparency</u>

Views For:

- Information asymmetry is a market failure, which needs to be corrected so that consumers can make informed choices about the service they use.
- Transparency requirements create a disincentive to violate remaining net neutrality rules; and make it easy to identify net neutrality violations.
- Transparency requirements will ensure that OTT-SPs have the requisite technical information for providing predictable services using TEL-SP infrastructure. For example, app developers need to know how the data for their apps will be treated.
- Transparency requirements increase consumer confidence in the operator.
- Transparency requirements will increase the effectiveness of the regulator.

Views Against:

- Transparency requirements will impose high regulatory costs on TEL-SPs.
- Transparency requirements may make the network more vulnerable to hackers by making operational data available.
- Transparency requirements could undermine the effectiveness of network management practices as it would inform people how to circumvent them.
- Consumers can't be expected to understand details of network management practices.

International Practices:

- Norwegian guidelines provide that "if the physical connection is shared with other services, it must clearly be stated how the capacity is shared between Internet traffic and other services".[2]
- The US open order 2015 states that "A person engaged in the provision of broadband Internet access service shall publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain Internet offerings."[3]
- The US Open Order of 2010 suggests disclosure of network practices (congestion management, application-specific behaviour, device attachment to network, security), performance characteristics (service description, impact of Specialised Services), and commercial terms (pricing, privacy policy and redress options)
- The US Open Order 2010 report notes that "The rule does not require public disclosure of competitively sensitive information or information that would compromise network security or undermine the efficacy of reasonable network management practices. For example, a broadband provider need not publicly disclose information regarding measures it employs to prevent spam practices at a level of detail that would enable a spammer to defeat those measures"

Recommendations:

TRAI should introduce a transparency requirement for standardised reporting of:

1. Network management practices;
2. Commercial terms of service;
3. Sharing of traffic between Internet Based Services and Specialised Services;
4. Exercise of exceptions to net neutrality;
5. Service information including privacy policy and redressal options.

- Networks may redact information that may compromise the security and stability of the network only if this information would not be available to a network security expert after reasonable effort.
- Reports should be available to the general public for free in a simple and accessible format.
- TRAI should compile and publish these reports.
- While transparency doesn't automatically result in better-informed consumer choice, since most consumers do not find network management practices easy to understand, it is a necessary cost to enable consumers to choose between competing TEL-SPs.

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?

Net Neutrality should include the following exceptions:

1) Reasonable Network Management
2) Specialised Services
3) Other public services/benefit/good/market failures exceptions

<u>Reasonable Network Management</u>

Views For:

- Given spectrum constraints (limited, fragmented and non-contiguous), network management practices for congestion management and maintaining quality of service are extremely important in India.
- Network management for maintaining the security, stability and integrity of the network are essential.
- Different applications and services require different quality of service. For example, real-time voice services require higher priority than messaging services. Similarly emergency health services may require preference over a gaming service.
- Network management practices can be personalised for each user based on user request (such as for parental control).
- Policy for network management has to be developed on a case to case basis.
- Network management may be required to deal with UCC, Spam, Denial of Service attacks etc

Views Against:

- Network management is a reasonable exception to net neutrality as long as it is not application or service specific.
- Network management should not involve deep packet inspection wherein the TEL-SP has traffic management rules based on content or application.
- TEL-SPs should not use network management to throttle services of competitors or small innovators.

International Practices:

- Under the Federal Communication Commission (FCC) order of March 2015, "Reasonable Network Management is an exception to the no-blocking rule, no-throttling rule, and no-unreasonable interference/disadvantage standard, ***but not to the rule against paid prioritization***."
- The US Open Internet order 2010 says that "Legitimate network management purposes include: ensuring network security and integrity, including by addressing traffic that is harmful to the network; addressing traffic that is unwanted by end users (including by premise operators), such as by providing services or capabilities consistent with an end user's choices regarding parental controls or security capabilities; and reducing or mitigating the effects of congestion on the network"
- Prior to Amendment 243, the European directive stated that "Reasonable traffic management measures shall be transparent, non-discriminatory, proportionate and necessary to a) implement a legislative provision or a court order, or prevent or impede serious crimes; b) preserve the integrity and security of the network, services provided via this network, and the end-users' terminals; c) prevent the transmission of unsolicited communications to end-users who have given their prior consent to such restrictive measures; d) minimise the effects of temporary or exceptional network congestion provided that equivalent types of traffic are treated

equally. Reasonable traffic management shall only entail processing of data that is necessary and proportionate to achieve the purposes set out in this paragraph."

- Netherlands law allows an exception to net neutrality "for the benefit of the integrity and security of the network, the service provider or the end user;"
- "As exceptions to the neutrality rule, reasonable network management activities should be consistent with international human rights standards regarding transparency, narrow tailoring, and proportionality. Wherever possible, traffic management practices should be content- and application-neutral. This is the most reliable way to ensure that traffic management is applied fairly and evenly, and that the ISP is not selecting which specific content or applications to favour or disfavour."[1]
- Open Internet NPRM, the Commission proposed that "open Internet rules be subject to reasonable network management, consisting of reasonable practices employed by a provider of broadband Internet access service to: (1) reduce or mitigate the effects of congestion in its network or to address quality-of-service concerns; (2) address traffic that is unwanted by users or harmful; (3) prevent the transfer of unlawful content; or (4) prevent the unlawful transfer of content."
- FCC 2015 order recognises unreasonable interference/disadvantage in addition to throttling and blocking: "We agree that a network management exception to the no-blocking rule, the no-throttling rule, and the no-unreasonable interference/disadvantage standard is necessary for broadband providers to optimize overall network performance and maintain a consistent quality experience for consumers while carrying a variety of traffic over their networks."
- FCC 2015 order states that the first filter for determining whether network management is reasonable could be "For a practice to even be considered under this exception, a broadband Internet access service provider must first show that the practice is primarily motivated by a technical network management justification rather than other business justifications. If a practice is primarily motivated by such an other justification, such as a practice that permits different levels of network access for similarly situated users based solely on the particular plan to which the user has subscribed, then that practice will not be considered under this exception"
- FCC 2015 order has adopted a case-by-case standard "We recognize the need to ensure that the reasonable network management exception will not be used to circumvent the open Internet rules while still allowing broadband providers flexibility to experiment and innovate as they reasonably manage their networks. We therefore elect to maintain a case-by-case approach. The caseby-case review also allows sufficient flexibility to address mobile-specific management practices because, by the terms of our rule, a determination of whether a network management practice is reasonable takes into account the particular network architecture and technology"

Recommendations:

- Network management should be a permissible exception to net neutrality.
- In the following cases, network management may be service, application or user specific:
  (i) for network security, stability and integrity.
  (ii) for end user security.
  (iii) at end-user request.
  (iv) for prevention of spam and unsolicited communications.
- All network management practices should be time bound and proportional.
- Network management rules for wireless may be stricter (or different from) than those for wireline.
- Network management rules must only be motivated with technical justifications rather business justifications. For example, network management may not specifically be applied to users with a particular tariff plan.
- Network management rules should be reviewed on a case-by-case basis (rather than ex-ante) to allow flexibility and innovation; and any review should take into account network architecture and technology.

Further, application agnostic rules and end user control are only indicative of reasonable network management.

- To deal with network congestion, TEL-SPs should be allowed to create classes of services (and rate them on a scale from say 0 to 7) to prioritise delivery of services; as long as the TEL-SP is able to establish a well defined rationale for prioritising one class of service over another.
- All network management practices which involve blocking, throttling, or prioritization of any service, class of service, or protocol must be transparently published, and made clear to customers, potential customers, and the regulator.
- Where the TEL-SPs are providing a shared public WiFi network such as at an airport, then throttling of certain classes of services (such as video streaming) may be permissible if it is causing degradation of other services.

Specialised Service:

The TRAI needs to recognise the concept of Specialised Services and use it as a construct that is applicable across different parallel issues under consultation such as VoIP regulation and Net Neutrality. Specialised Services refers to services provided on a network that is either physically distinct from the Internet using different pipes or logically distinct from the Internet using access controls over the same pipes. Thus all services provided over a Closed Electronics Communications Network (CECN), or any other network not connected to the Internet, would be called Specialised Services. Accordingly, facility based VoIP services or managed VoIP services (including VoLTE) would be classified as Specialised Services. Similarly, the concept of specialised services would be applicable to services such as remote surgeries, self driving cars etc that demand a higher QoS which the best efforts delivery over the Internet cannot guarantee.

Views For:

- Net neutrality cannot be applied to traditional telecommunications services that have now migrated to an IP based infrastructure; For example, PSTN calls (VoLTE) are expected to deliver high quality of service and cannot be treated equivalent to Skype.
- TEL-SPs should be free to use their networks to provide any services that require higher quality of service as long as they keep such services logically distinct from Internet Based Services.
- Specialised Services can help satisfy the need to guarantee the quality of certain forms of communication such as emergency health services.
- TEL-SPs should be able to prioritise their own services on their own infrastructure as Internet Based Services are competing with Specialised Services using the same IP architecture.
- "Specialised Services for data-intensive or time-sensitive applications would allow operators to charge for providing guaranteed levels of service and hence would provide the certainty and the financial incentives that are needed to justify infrastructure investments",[2]

Views Against:

- There is a fear that TEL-SPs may expand the scope of "Specialised Services" if the term is not properly defined.
- If high quality Specialised Services take up a large chunk of existing bandwidth, network operators may downgrade the 'standard' open internet service, leading to poorer service for those who cannot afford to pay more.

International Practices:

- FCC open order report 2010 recognises that "Our rules against blocking and unreasonable discrimination are subject to reasonable network management, and our rules do not prevent broadband providers from offering specialized services such as facilities-based VoIP."

- FCC open order 2010 states that "The "specialized services," such as some broadband providers' existing facilities-based VoIP and Internet Protocol-video offerings, differ from broadband Internet access service and may drive additional private investment in broadband networks and provide end users valued services, supplementing the benefits of the open Internet."
- Amendment 236 in EU states that "Providers of internet access, of electronic communications to the public and providers of content, applications and services shall be free to offer Specialised Services to end-users. Such services shall only be offered if the network capacity is sufficient to provide them in addition to internet access services and they are not to the detriment of the availability or quality of internet access services. Providers of internet access to end-users shall not discriminate between functionally equivalent services and applications."
- In Netherlands, the concept of Specialised Services is not included. Reason stated is, by restricting the scope of application of net neutrality rules to internet services, it is not necessary to rely on the concept of Specialised Services to protect the functioning of managed, non-Internet Based Services. Both the open internet and the functioning of non-Internet Based Services are better guaranteed without defining Specialised Services.

Recommendations:

- Specialised Services should be recognised as an exception to net neutrality.
- Quality of service to Specialised Services should not be secured at the expense of Internet Based Services.
- A service for which best-efforts delivery is feasible may not be classified as a specialised service.

---

[1] http://www.eurolinc.eu/IMG/pdf/NetNeutrality-Rapport.pdf, accessed on 20 April, 2015.

[2] Bibilo briefing net neutrality in Europe

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

<u>Scope of TRAI Powers & Instruments</u>

It is suggested that TRAI refrain from providing recommendations on regulation of non-communication OTT players. The mandate of regulating such services is that of the Parliament by amending the IT Act and its rules thereunder. While recognising the limitations of its own mandate, TRAI may recommend the need for a new converged regulator and a new converged legislation combining various aspects of Information Technology, Telecommunications and Broadcasting. The issues brought to the forefront by the rise of OTT services require a major overhaul of many related legislations and cannot be entirely addressed by incremental efforts of TRAI.

It is strongly urged that OTT-SPs should be regulated by instruments other than licensing. Preferably, OTT-SPs should be regulated through instruments such as the IT Act and its Rules thereunder. This is an imperative requirement for innovation on the Internet to continue to prosper. However, "communications" OTT-SPs should be encouraged to voluntarily adopt the Unified License through regulatory and economic incentives. This can possibly encouraged by introducing a trimmed down version of the Unified License with low regulatory compliance costs and zero revenue sharing. Such a voluntary license would authorise OTT-SPs to terminate calls on the PSTN. In return, the license could impose slightly higher requirements for interception than presently imposed by the Information Technology Act.

The regulations for OTT-SPs and TSPs cannot be exactly the same. However, there can be reasonable parity in the regulations that govern the two. Such reasonable regulatory parity can be achieved even if TSPs are regulated by licenses and OTT-SPs are regulated by instruments other than licensing.

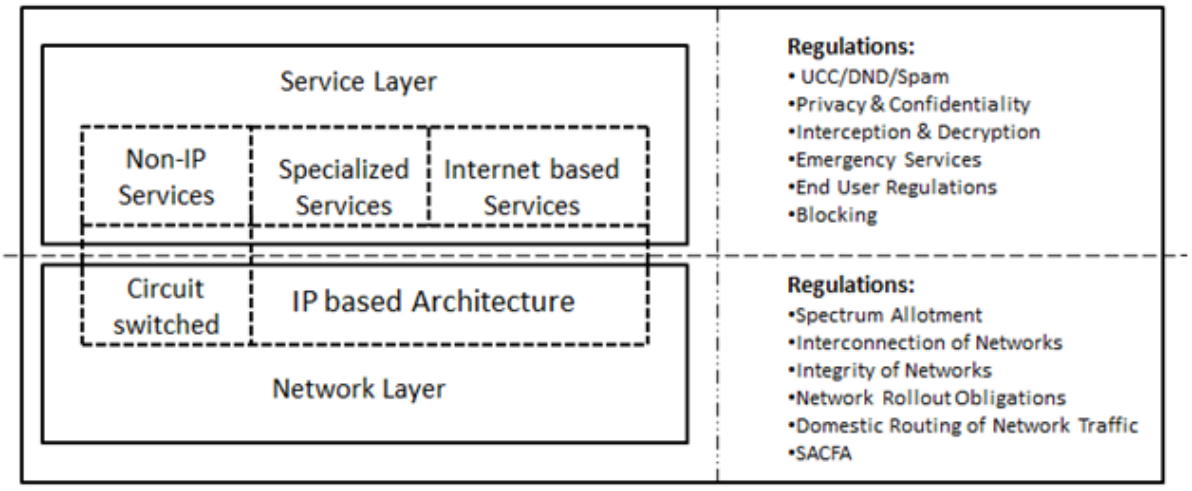
Recommended Regulatory Principles

Introduction to Recommended Framework of Principles

In this section, we propose a set of principles that collectively prescribes the framework for intervention by TRAI. The framework provides guidelines for (i) introducing reasonable regulatory parity between functionally equivalent services provided by TEL-SPs and OTT-SPs; and (ii) introducing net neutrality along with details of its different components and exceptions. Both interventions are closely interrelated and should not be considered independently. In accordance with this objective, the principles are categorised into three groups. The first group is a general set of principles that apply to both interventions. The second group is a set of principles on introducing regulatory parity. The third group is a set of principles on introducing net neutrality.

The framework adopts a two-layered approach. The first layer comprises of network and infrastructure (collectively called the Network Layer). The second layer comprises of services and applications (collectively called the Application/Service Layer). The framework further divides the second layer into "Non-IP Services", "Specialised Services" and "Internet Based Services". TEL-SPs operate over both the Network Layer and the Application Layer. Traditional services such as PSTN voice calls provided over a circuit switched network are referred to as Non-IP Services. The concept of "Specialised Services" is borrowed from the European Union. Practically, the term "Specialised Services" refers to traditional services that have migrated to IP networks (that are not interconnected with the Internet) such as facilities-based VoLTE calls to PSTN and IPTV. This concept is introduced to envision reasonable regulatory parity between functionally equivalent "Non-IP Services", "Specialised Services" and "Internet Based Services". In the framework, "Specialised Services" is also recognised as an exception to net neutrality. A short note with various definitions and critiques of "Specialised Services" is provided in Appendix 1.

Fig-2: Layered Framework with Corresponding Regulations



Principles Comprising Recommended Framework

Group 1 - General Principles

1. **Principle 1**: The Network Layer and Application Layer of TEL-SPs should be delinked; or deemed to be distinct for the purpose of this consultation.
   Explanations:
   i. While OTT-SPs operate only in the Application Layer, TEL-SPs operate both in the Network Layer and the Application Layer ;
   ii. Active infrastructure (including spectrum) is a part of the Network Layer;
   iii. SMS, PSTN voice calls, OTT applications, VAS services etc are a part of Application Layer.

2. **Principle 2:** Services in the Application Layer should be sub-classified into "Non-IP Services", "Specialised Services" and "Internet Based Services".[1]
   a. Traditional services provided over a non-IP based architecture (such as circuit switched calls) should be classified as "Non-IP Services".
   b. Services provided over an IP based architecture in a closed electronic communications network (i.e. not interconnected with the internet or relying on strict admission control) including facility-based services should be classified as "Specialised Services" (if they demonstrate the need for special treatment over and above the "best efforts" delivery guarantee possible over the Internet).
      Explanations:
      i. Concept of Specialised Services is borrowed from the European Union to refer to facility based services that have migrated to an IP architecture. Refer to different definitions of "Specialised Services" in Appendix 1.
      ii. Facility based services such as managed VoIP calls or IPTV services provided by TEL-SPs would be a part of "Specialised Services".
      iii. Voice over LTE/IP calls terminating on the PSTN would be treated as "Specialised Services" since they operate over a network distinct from the internet; even if they share the same network infrastructure - it relies on strict admission control. In comparison, voice/video calls provided using internet data over LTE would be treated as "Internet Based Services".
      iv. A regular Internet service must demonstrate a rational nexus between the differential treatment and its need in the form of demonstrating that "best efforts" delivery of IP packets do not suffice for the application or service.
   c. Services provided over the internet should be classified as "Internet Based Services". Such classification depends on the nature of the service and not the provider of the service: "Internet Based Services" may be provided by OTT-SPs or by TEL-SPs.
      Explanations:
      i. OTT applications would automatically be classified as Internet Based Services, unless it has specifically been classified as a "specialised service".
      ii. Voice and video calling over the Jio Chat application released by Reliance Jio (a TEL-SP) would be classified as an internet based service.

Group 2 - Regulatory Parity Principles

1. **Principle 3:** The Network Layer *may* be regulated by way of licensing.
2. **Principle 4:** Non-IP Services and Specialised Services *may* be regulated by way of licensing.[2]
3. **Principle 5:** Internet Based Services *should* be regulated by instruments other than licensing. Such instruments should preferably be in the form of legislations like the IT Act and its rules thereunder.

4. **Principle 6:** There needs to be regulatory parity between communications oriented "Internet Based Services" provided by OTT-SPs and TEL-SPs.
5. **Principle 7:** ***There needs to be reasonable regulatory parity between functionally-equivalent "Internet Based Services", "Non-IP Services" and "Specialised Services" (refer Table in response to Questions 4,5,6)***. However, the specialised nature of Specialised Services may require substantially different treatment, which should be determined on a regulation to regulation and a service to service basis.
6. **Principle 8:** Arguments for regulatory parity between the "Network Layer" and "Internet Based Services" are incorrect as the two belong to different layers.
7. **Principle 9:** Regulations for "Internet Based Services" may create sub-classifications such as communication services, market services and aggregation services, provided there is a reasonable nexus between the classification and the objective sought to be achieved by the regulation.[3]
8. **Principle 10:** Regulations for "Internet Based Services" need to be such that they promote innovation by small entrepreneurs and innovators while also incorporating concerns related to security, lawful interception and removal of unlawful content.
9. **Principle 11:** Regulatory parity may be sought to be arrived at by decreasing the existing regulations on TEL-SPs and not merely by increasing regulation on OTT-SPs.

Group 3 - Net neutrality Principles

1. **Principle 12:** Net neutrality should be codified[4] and enforced:
    a. Networks should be required to deliver all Internet traffic on a best effort basis without discrimination on the basis of protocol, port number, content, device, service, origin/sender or destination/receiver.
    b. No negative discrimination by the TEL-SPs shall be allowed in the form of throttling, or blocking or paid prioritisation subject to the contextualisation described in Section 5.
    c. OTTs should not be required to pay the terminating network for termination of traffic.
    d. Publish transparency reports in exercise of all reasonable exceptions to net neutrality.
    e. Internet Based Services should not be degraded as a result of Specialised Services[5].
2. **Principle 13:** There are certain reasonable exceptions to net neutrality including:
    a. Compliance with orders given by statutory bodies of law and court decisions.
    b. Specialised Services (Alternately: net neutrality should only be enforced for Internet Based Services)[6]
    c. Reasonable network management
        i. Discrimination for the sake of network management is only permissible if[7]:
            1. there is an intelligible differentia between the classes which are to be treated differently, and
            2. there is a rational nexus between the differential treatment and the aim of such differentiation, and
            3. the aim sought to be furthered is legitimate, and is related to the security, stability, or efficient functioning of the network, or is a technical limitation outside the control of the TEL-SP, and
            4. the network management practice is the least harmful manner in which to achieve the aim.
        ii. Measures based on direct request from the end user. *Explanation*: At user request, the TEL-SP may block porn content.
        iii. Certain forms of positive discrimination may be allowed, subject to them meeting strict conditions such that they do amount to negative discrimination.

1. These should generally not be on the basis of content- or source/destination, since that in general would have negative impact on competition, consumers, and network openness and diversity.
2. The only situation in which such positive discrimination (including paid and unpaid zero-rating) may be allowed is if it does not harm competition and consumers, and care is taken to ensure it only minimally harms openness and diversity.
3. Paid zero-rating or zero-rating on the basis of a deal with an OTT must be strictly regulated.[8]
4. Other forms of zero-rating may be permitted as long as the regulator ensures it doesn't occur alongside TEL-SPs raising the cost of general Internet data packs for consumers (by raising prices or decreasing data caps).[9]

---

[1] Specialised Services is a construct imported from the European Union & United States

[2] The current regime of a single license for the Network Layer and Specialised Services can continue.

[3] For example, regulations relating to emergency communications have a reasonable nexus with the category "communications services"

[4] This should be codified in the license agreement between the Central Government and Network Providers (TEL-SP).

[5] QoS parameters that are monitored by TRAI need to be disaggregated as TEL-SPs can not guarantee end to end QoS for Internet Based Services.

[6] Same difference as that between the Dutch legislation and the European Commission's proposal. See blogs.lse.ac.uk/mediapolicyproject/2014/04/04/why-not-go-dutch-and-protect-net-neutrality-without-defining-specialised-services/

[7] Examples: For security and integrity of the network including dealing with undesirable traffic such as service attacks, malware, port scans etc.; For prevention of unsolicited communication.; and Application/service specific congestion management in emergency circumstances directly related to the stability of the network.

[8] This regulation may be in terms of access to all OTTs to the marketplace, on non-discriminatory and standard terms;
This regulation may be in terms of what additional content will have to be zero-rated (e.g., one level of hyperlinks from zero-rate content);
This regulation may be in terms of requiring zero-rating of all of Internet content for a specific period of time, etc.

[9] For instance: A TEL-SP may voluntarily offering special "top-up packs" for traffic to and from specific OTT services, may offer zero-rated access to the Internet in exchange for viewing of advertisements, may offer zero-rated access to the Internet at low-speeds, creating an incentive for users to pay for higher speeds; or it may voluntarily zero-rate traffic from local Internet Exchange Points or from settlement-free peering arrangements insofar as the TEL-SP incurs lower costs from such traffic. These practices need to be disclosed by TEL-SPs and need to be monitored by the regulator.

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.

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

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

There are regulatory imbalances between functionally equivalent services provided by OTT-SPs and TEL-SPs. We present below a table that suggests interventions to introduce reasonable regulatory parity between functionally equivalent "Internet Based Services", "Non-IP Services" and "Specialised Services". However, it is recognised that the nature of specialised services may require substantially different treatment, which should be determined on a

regulation to regulation and a service to service basis. It also recognised that arguments for regulatory parity between the "Network Layer" and "Internet Based Services" are incorrect as the two belong to different layers (For example: TSPs claim that they have incurred cost for purchasing spectrum while OTTs have not).

The consultation paper highlights the regulatory imbalance between "Internet Based Services", "Non-IP Services" and "Specialised Services". However, the consultation paper incorrectly posits that "Internet Based Services" provided by OTT-SPs are completely unregulated. The following table attempts to outline the different regulations for OTT-SPs and TEL-SPs. The table also attempts to delink the regulations attributable to the network and service layers of TEL-SPs. The table also identifies the areas where there is regulatory imbalance and suggests a recourse.

Regulations	**OTT-SPs (Service Layer) Internet Based Services**	**TEL-SPs (Service Layer) Non-IP and Specialised Services**	**TEL-SPs (Network Layer)**	**Layer to which the regulation belongs**	**Regulatory Imbalance?**	**Suggested recourse for correcting imbalance; or justification for maintaining present imbalance.**
UCC/DND/Spam	No clear legislation on spam. Previously partially covered by Section 66A(c) of IT-Act, which has now been struck down by the Supreme Court	TRAI Regulation on 200 SMS per day.[1] TRAI Regulation on UCC[2].		Service	Yes	Spam & UCC over OTT services need to be regulated. However, the mandate to regulate spam is that of the parliament by creating a new act or amending the IT-Act, and not that of TRAI. TRAI may however recommend to the Government to consider an amendment to such effect in the IT-Act.
Privacy and Confidentiality	Section 43A of IT-Act	License Agreements (UASL[3], UL[4])		Service	No	Section 43A is reasonably at par with clause 39.2 of the UASL. Additionally, there is a Privacy Bill presently under consideration by the Government that also addresses privacy concerns relating to OTTs.
Spectrum Allotment including Auctions and Revenue Sharing			Wireless Operating License r/w License Agreements (UASL, UL) r/w NIA	Network	No	There is no regulatory imbalance as the service layers of OTT-SPs and TEL-SPs are treated at par. *See principle 7.*
Interconnection of Networks			TRAI Regulations; Reference Interconnect Order (RIO); License Agreements (UASL, UL).	Network	No	There is no regulatory imbalance as the service layers of OTT-SPs and TEL-SPs are treated at par. *See principle 7.*
Interconnection of Services	No regulation.	TRAI Regulations; Reference Interconnect Order (RIO); License Agreements (UASL, UL).		Services	Yes	It should remain mandatory for OTT-SPs to get a Unified License for interconnecting Internet Telephony with the PSTN/PMLN. Alternatively, a trimmed down voluntary licensing arrangement could be created that allows OTT providers to interconnect with PSTN and terminate calls on the PSTN. Such a license would create slightly higher regulatory compliances for interception etc. OTT services maybe mandated to interconnect with each other if technically feasible and regulatorily desirable for a competitive marketplace.
Security & Integrity of Networks			License Agreements (UL)[5]	Network	No	There is no regulatory imbalance as the service layers of OTT-SPs and TEL-SPs are treated at par. *See principle 7.*

Interception & Decryption	Section 69 of IT-Act	Section 5 of Tele-Act; License Agreements (UASL, UL).		Services	Yes	While TEL-SPs are required to create infrastructure and be technically compliant with lawful interception requests, OTT-SPs are not required to be technically prepared for interception; and may not be technically capable of honouring an interception request. There is need to move towards parity here. Ideally, the burden on TEL-SPs should be substantially decreased. The other option, though infeasible in most instances, is to substantially increase interception requirements for those communication OTT-SPs that are based on server-side encryption and have achieved a minimum critical mass, wherein whether an OTT-SP has reached critical mass (on the basis of minutes of usage, data consumption or subscriber base) would be determined by TRAI. Those OTT-SPs that provide lawful interception in other countries but refuse to comply in India should be blocked.
Subscriber Verification	No regulation.	License Agreements (UASL[6], UL[7]).		Services & Networks	Yes	Subscriber identity verification can effectively happen only at the network layer, given the fact that most service-layer platforms do not have the means of tying a user's physical identity with their virtual existence. There are some OTT-SPs that bind their users to a network-layer identification like their PSTN number (e.g., WhatsApp), in which case the demand for subscriber verification gets addressed despite the lack of regulatory parity.
Network Rollout Obligations			License Agreements (UASL, UL)[8].	Network	No	There is no regulatory imbalance as the service layers of OTT-SPs and TEL-SPs are treated at par. *See principle 7.*
Permission to terminate voice calls on the PSTN	No. ISP license prohibits connectivity of Internet Telephony with domestic PSTN[9]	Yes. License Agreements (UASL, UL[10]).		Service	Yes	It should remain mandatory for OTT-SPs to get a Unified License for interconnecting Internet Telephony with the PSTN/PMLN.
Emergency and Public Utility Services	No regulation.	License Agreements (UASL, UL).[11]		Service	Yes	Those OTT-SPs that reach a critical mass should be mandated to provide these emergency services. For example, Skype provides emergency services in 4 countries including the United Kingdom. Similar requirements should be imposed by India as well.
Quality of Service	No regulation	TRAI Regulation on Quality of Service		Service and Network	Yes	QoS delivered by OTT services is not fully in the control of the OTT-SP, unless they launch a specialised service that provides QoS guarantees. In such a case, they may be subject to appropriate regulation.
Bulk Encryption Prohibition	No regulation	License Agreements (UASL[12], UL[13]).		Service	Yes	This regulation needs to be removed completely for both TEL-SPs and OTT-SPs.
Domestic Routing of Network Traffic			License Agreements (UL[14])	Network	No	There is regulatory imbalance between UL (Access) and ISP License; However this imbalance is between two kinds of licenses and does not involve the OTT-SPs since switching happens at the network layer.
End User Regulation (Cyber Crimes)	Section 43 of IT-Act	Section 43 of IT-Act		Service	No	Section 43 deals with end user cyber crimes and therefore equally applies to end users of OTT-SPs and TEL-SPs.
Blocking	Section 69A of IT-Act	License Agreements (ISP, UL)[15], (UASL)[16]		Service	No	There is reasonable parity.
Contribution to USOF			Section 9A of the Telegraph		No	There is no regulatory imbalance as the service layers of OTT-SPs and TEL-SPs are treated at par. *See*

			act			*principle 7.*
SACFA		License Agreements (UASL[17], UL[18])		Network	No	There is no regulatory imbalance as the service layers of OTT-SPs and TEL-SPs are treated at par. *See principle 7.*

---

[1] The Telecom Commercial Communications Customer Preference Regulations,"The Authority has mandated the service providers to implement a solution in their networks which will not allow sending of more than 200 SMS with similar 'signature' in one hour from any source or number, other than from a registered telemarketer or transactional message sending entity or a number exempted by the Authority."

[2] http://www.trai.gov.in/content/VerReg/57_0_0.aspx, accessed on 17 April, 2015.

[3] 39.2 Subject to conditions contained in these terms and conditions, the LICENSEE shall take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the SERVICE and from whom it has acquired such information by virtue of the SERVICE provided and shall use its best endeavors to secure that :a) No person acting on behalf of the LICENSEE or the LICENSEE divulges or uses any such information except as may be necessary in the course of providing such SERVICE to the Third Party; and b) No such person seeks such information other than is necessary for the purpose of providing SERVICE to the Third Party. Provided the above para shall not apply where: a) The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or b) The information is already open to the public and otherwise known.
39.3 The LICENSEE shall take necessary steps to ensure that the LICENSEE and any person(s) acting on its behalf observe confidentiality of customer information.
39.4 The LICENSEE shall, prior to commencement of SERVICE, confirm in writing to the LICENSOR that the LICENSEE has taken all necessary steps to ensure that it and its employees shall observe confidentiality of customer information
41.4 The LICENSEE shall ensure protection of privacy of communication and ensure that unauthorized interception of messages does not take place.

[4] 37.2 Subject to terms and conditions of the license, the Licensee shall take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the Service and from whom it has acquired such information by virtue of the Service provided and shall use its best endeavors to secure that:
a) No person acting on behalf of the Licensee or the Licensee divulges or uses any such information except as may be necessary in the course of providing such Service to the Third Party; and
b) No such person seeks such information other than is necessary for the purpose of providing Service to the Third Party.

[5] 39.7 The LICENSEE shall induct only those network elements into its telecom network, which have been got tested as per relevant contemporary Indian or International Security Standards

[6] 41.14 … The LICENSEE shall ensure adequate verification of each and every customer before enrolling him as a subscriber; instructions issued by the licensor in this regard from time to time shall be scrupulously followed…
41.15 A format would be prescribed by the LICENSOR to delineate the details of information required before enrolling a customer as a subscriber. A photo identification of subscribers shall be pre-requisite before providing the service.

[7] 39.17 (i) The Licensee shall ensure adequate verification of each and every customer before enrolling him as a subscriber; instructions issued by the Licensor in this regard from time to time shall be scrupulously followed. The Licensee shall make it clear to the subscriber that the subscriber will be responsible for proper and bonafide use of the service.
39.22 (i) Utmost vigilance should be exercised in providing bulk connections for a single user as well as for a single location. Provision of 10 or more connections may be taken as bulk connections for this purpose….

[8] Refer section 34 in License Agreement for Provision of Unified Access Services after Migration from CMTS and section 4 in License Agreement for Unified License

[9] v) The Licensee is not permitted to have PSTN/PLMN connectivity. Voice communication to and from a telephone connected to PSTN/PLMN and following E.164 numbering is prohibited in India.

[10] The Licensee can also provide Internet Telephony, Internet Services including IPTV, Broadband Services and triple play i.e voice, video and data. While providing Internet Telephony service, the Licensee may interconnect Internet Telephony network with PSTN/PLMN/GMPCS network. The Licensee may provide access service, which could be on wireline and / or wireless media with full mobility, limited mobility and fixed wireless access.

[11] 29.1 The licensee shall provide independently or through mutually agreed commercial arrangements with other Service Providers all public utility services including TOLL FREE services such as police, fire, ambulance, railways/road/air accident enquiry, police control, disaster management etc. While providing emergency services such as police, fire, ambulance etc. it shall be ensured that such calls originated shall be delivered to the control room of the concerned authority for the area from where call is originated.

[12] 41.12 The LICENSEE shall not employ bulk encryption in its network. Any encryption equipment connected to the LICENSEE's network for specific requirements has to have prior evaluation and approval of the LICENSOR or officer specially designated for the purpose. The LICENSEE shall be responsible for ensuring privacy of communication on its network and also to ensure that unauthorized interception of message does not take place.

[13]
37.1 The Licensee shall not employ bulk encryption equipment in its network. Licensor or officers specially designated for the purpose may evaluate any encryption equipment connected to the Licensee's network.

[14]
4.5 Location of switches and other elements.

[15]
7.11, 34.24 … In the interest of national security or public interest, the ISPs shall block Internet sites and / or individual subscribers, as identified and directed by the Licensor from time to time.

[16]
There is no such clause in UASL.

[17]
43.3 Site clearance in respect of fixed stations and its antenna mast shall be obtained from the WPC Wing for which the applicant shall separately apply to the Secretary, Standing Advisory Committee on Frequency Allocations (SACFA) WPC Wing in a prescribed application form.

[18]
30.11 (iii) For use of space segment and setting up and to start operating the Earth Station etc., Licensee shall directly coordinate with and obtain clearance from Network Operations Control Centre (NOCC), apart from obtaining SACFA clearance and clearance from other authorities.

Additionally, TRAI should take an holistic view based on other issues being discussed in:

- Consultation on VoIP including QoS, interconnection, numbering etc
- Consultation on Cloud Computing including licensing of cloud services, data localisastion, numbering etc

since there are considerable overlaps between these consultations. A piecemeal approach will substantially increase the complexity of the legal regime.

Appendix 1 - Note on Specialised Services

Different definitions of Specialised Services:

BEREC (2011):
"Specialised services" are electronic communications services that are provided and operated within closed electronic communications networks using the Internet Protocol. These networks rely on strict admission control and they are often optimised for specific applications based on extensive use of traffic management in order to ensure adequate service characteristics.

BEREC (2012):
Specialised services are usually designed to provide guaranteed characteristics of end-to-end connections (e.g. quality of service, availability and/or security). These characteristics are generally stated in contractual arrangements. Technically, specialised services typically rely on access restrictions and extensive use of traffic management techniques or strictly enforced capacity planning and provisioning.

Digital Europe[1]:
"Specialised services" 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.

Dynamic Coalition on net neutrality:
"Specialised services" are electronic communications services that are provided and operated within closed electronic communications networks using the Internet Protocol, but not being a part of the Internet. The expression "closed electronic communications networks" refers to networks that rely on strict admission control.

Amendment 235:
"Specialised service" means an electronic communications service optimized for specific content, applications or services, or a combination thereof, provided over logically distinct capacity, relying on strict admission control, offering functionality requiring enhanced quality from end to end, and that is not marketed or usable as a substitute for internet access service.

Conditions to the application of Specialised Services:

- "Quality of service to specialised services is not secured by giving these services an explicit higher priority level than the internet based services, but rather by having adequate capacity reserved for the specialised services without this being done at the expense of Internet traffic."
- Providers of content, applications and services and providers of electronic communications should therefore continue to be free to conclude specialised services agreements on defined levels of quality of service as long as such agreements do not impair the quality of internet access service.
- Amendment 236 states that "Providers of internet access, of electronic communications to the public and providers of content, applications and services shall be free to offer specialised services to end-users. Such services shall only be offered if the network capacity is sufficient to provide them in addition to internet

access services and they are not to the detriment of the availability or quality of internet access services. Providers of internet access to end-users shall not discriminate between functionally equivalent services and applications."

---

[1] http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=721&PortalId=0&TabId=353