Responses to the Pre-Consultation Paper on Net Neutrality

We thank TRAI for initiating this pre-consultation process on Net Neutrality. However, as the earlier consultation process on Regulatory Framework for Over-the-top (OTT) services had questions related to Net Neutrality, we hope that the responses submitted for that consultation will also be considered while analyzing this issue. Our responses to this consultation paper are drawn to a large extent from the earlier consultation process as the issues dealt with are largely similar.

One of the basic legal protections for the freedom of the market embedded in the common law is the non-discriminatory principle of public carriage. If firms providing transport services to the public are able to discriminate among shippers or receivers of goods, they can profit hugely, at the expense of other market participants generally, their own cartel allies excepted. So from ferrymen in medieval England to railroad and trucking companies in the 20th century, prohibiting anti-competitive discrimination in transport services for the public is basic to the fair working of the market.

Telecommunications services are not different in this respect from other forms of transport. Regulators in the 20th century dealt with telephone and other such services on a common-carriage basis, in order to prevent anti-competitive collusion. One aspect of the group of ideas sometimes misleadingly called, all together, "network neutrality," is the principle of prohibiting anti-competitive routing practices. As the recent experience of the US Federal Communications Commission has shown, management of a fair Internet is now as fundamental to the free market as the prohibition by other regulators of anti-competitive practices in other forms of transport. The FCC's imposition of common-carriage rules for Internet service providers is a victory for the public interest after a decade of attempts by industry to capture the regulators, to prevent this very outcome.

The integrity of the network — that it provides one indivisible opportunity for everyone connected to it — is its most important feature. As a tool of social development, the Internet allows people with little capital equipment but plenty of ingenuity to build effective businesses from zero. But only if other people can ‘find’ them on the Internet and receive the services they are offering.

Question 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?

We recommend that a neutral Internet be guided by the following principles:

1. *No Application Based Discrimination*: TSPs should not discriminate Internet traffic based on content, any applications or classes of applications or services
2. *No Paid Prioritization*[1]: TSPs should not be allowed to favor some content or traffic over another for any consideration, no "fast lanes" should be allowed.
3. *No Throttling or Blocking*: All content should be treated equally and TSPs should not intentionally slow down the speed of some content or speed up others based on the type or TSP's preference.
4. *Transparency in Traffic Management*: The traffic management principles adopted by the TSPs should be transparent and application-agnostic and should primarily be used to achieve a legitimate traffic management purpose and not a discriminatory commercial purpose.
5. *No Deep Packet Inspection*[2]: No DPI should be allowed unless for specified reasons mandated by law and that should be made transparent.
6. *No Zero Rating*: The practice of Zero rating where content providers pay TSPs to provide end-users free or subsidized access to their websites should be banned.

Beyond rules that prevent TSPs from blocking applications or content, non-discrimination rules are a key component of any net-neutrality regime. The Regulator should encourage a non-

1 Paid prioritization is a financial agreement in which a content provider pays a provider of Internet services to essentially jump the data queue at congested points. The practice also involves internet providers prioritizing their own content or that of an affiliate over data from a competing edge provider. With finite bandwidth capabilities, the creation of “fast lane” entails the implicit creation of an accompanying “slow lane” for other data not being sped up. Ultimately only a limited group of providers are able to pay for such priority, resulting in anti-competitive practices, hindering innovation and undermining of consumer rights.

2 DPI is the form of packet filtering that examines the data part of a packet as it passes inspection point, searching for protocol non-compliance, viruses, spam, intrusions or defined criteria to decide whether the packet may pass or if it needs to be routed through a different destination, or , for the purpose of collecting statistical information. DPI enables advance network management, data mining, blocking, prioritizing traffic and allows providers of Internet services to gather statistical information about use patterns by user group. Internet access providers can use this to implement tiered service plans and tailor their offerings to individuals subscribers based on their usage, which in turn increases their Average Revenue Per User. Service providers may thus have profit motives to analyze what their subscribers are viewing, and be able to use such information to their financial advantage.

discrimination rule that bans all application-specific discrimination.[3]

We believe that the term "Network Neutrality" – although popular – is misleading and provides excuses that purport to justify discrimination over the network. We recommend using the term "Network Integrity". Semantics aside, whether the usage is neutrality or Integrity, it must be defined clearly. Any rules that are adopted must ensure that user choice is preserved, do not discriminate on the basis of kind of applications, do not restrict freedom of speech and expression, keep the entry barriers low and promote innovation.

As observed by Professor Tim Wu, Professor of Law at Columbia University, in his seminal paper on net neutrality, the argument for a neutral Internet must be understood as the concrete expression of a system of belief about innovation, whose adherents view the innovation process as a survival-of-the-fittest competition among developers of new technologies.[4] Models of development must not vest control in any initial prospect-holder, private or public, who is expected to direct the optimal path of innovation, minimizing the excess of innovative competition.[5] This innovation theory, according to J H Saltzer et. al., is embodied in the end-to-end network design argument, which in essence suggests that networks should be neutral as among applications.[6] The Internet Protocol suite was designed to follow the end-to-end principle, and is famously indifferent to the physical communications medium below it and the applications running above it. The argument for net neutrality therefore, is anchored in the protection of certain core characteristics of the Internet that have played central roles in making it a quintessential tool for information exchange in the 21st century. It is also important to remember, when speaking of net neutrality from a regulatory perspective, that the spectrum over which Internet data is transmitted is a scarce natural resource, and as such brings with it an obligation on the State to ensure that a non-discriminatory method is adopted for its distribution and alienation, which would necessarily result in protection of national/public interest.

There are several ways in which net neutrality may be compromised by private action, including:

---

3 Discrimination is application-specific if the discrimination is based on the specific application or content (e.g. Skype is treated differently from Google Voice), or based on classes of applications or content (e.g. Internet telephony is treated differently from a mail)

4 Tim Wu, *Network Neutrality, Broadband Discrimination*, Journal on Telecom and High Tech Law, available at: http://www.jthtl.org/content/articles/V2I1/JTHTLv2i1_Wu.PDF, last accessed on July 2, 2016

5 Ibid.

6 J H Saltzer et al., *End-to-End Arguments in System Design*, available at: http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf, last accessed on July 2, 2016

- Arbitrarily blocking competing online content and services
- Throttling or slowing down access to the content and services of competitors
- Providing higher quality of access to one's own content and services and those of commercial partners
- Zero-rating particular content and services by discounting applicable data charges so as to promote their adoption and use over others
- Imposition of differential tariffs on certain content and services in relation to others

Regulatory prohibition of the above practices is necessary to ensure continued respect for the principle of net neutrality within India.

Question 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?

When considering 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, there are several important issues to consider. Traffic management has a direct impact on issues like access, privacy, freedom of speech. It is imperative for TRAI that it must thoroughly assess citizen impact of net neutrality and traffic management in terms of its long term as well as short term effects.

An approach towards traffic management with the prime focus being provision of better quality of services, would not necessarily bring benefits to consumers who do not have much control over the speeds that they receive, including consumers in rural areas who are restricted by technology or low-income consumers who cannot pay for better quality of service. Such traffic management practices will lead to the Internet being divided into different tiers, based on quality of services while also affecting the overall baseline quality of services, being degraded in favor of higher tiers for consumers who can afford to pay for them.

This would lead to low-income consumers not having the same choice of services, and could find that the quality of service that they receive is negatively affected by prioritization in favor of consumers who are able to pay for a better quality of service. Such prioritization while affecting the

baseline quality of services being degraded will also affect the low-income consumer's overall experience of what the Internet is, having a much larger impact in a country like India where access to itself is a big issue. Thus, an approach towards traffic management with the prime focus being provision of better quality of services could lead to TSPs discriminating between different income-consumers & affecting the neutral character of the Internet.

It may also be noted that in the longer term this approach may create barriers to entry for providers that wish to develop and deliver new content and services but cannot pay telecom operators for prioritization of their content, which could stifle innovation.

Another issue[7] includes the whole public sector on the Internet. A huge number of Government departments and agencies are putting forms & information online. In future, it may extend to video content that explains important public information. Other entities include publicly funded institutions, which also use the Internet to distribute their content & services. Thus, traffic management could also impact how citizens access these services in the future.

Moreover, if Quality of Service (QoS) based traffic management is ever allowed, it should allow application-agnostic discrimination. Studies show that application-agnostic discrimination does not constrain the evolution of the network more than is necessary to reach the goals of network neutrality regulation.[8] It provides room for networks to evolve in that it allows network providers to offer certain (though not all) forms of Quality of Service. In particular, it allows network providers to offer different classes of service if they meet the following conditions:

- The different classes of services are offered equally to all applications and classes of applications;
- The user is able to choose whether and when to use which class of service;
- The network provider is allowed to charge only its own Internet service customers for the use of the different classes of services.

A provider of Internet services, who is allowed to charge for QoS has an incentive to degrade the

7 Ofcom's discussion document on Traffic Management & 'net neutrality', available at: http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf

8 Network Neutrality and Quality of Service- What a Non-Discrimination Rule Should Look Like" by Barbara Van Schewick

quality of the baseline, best-effort service to motivate users to pay for an enhanced type of service. To mitigate this problem, any network neutrality regime that allows network providers to charge for QoS should require the regulatory agency in charge of enforcing the network neutrality rules to monitor the quality of baseline services and set minimum quality standards if the quality of the baseline service drops below appropriate levels.

The Internet's original architecture was based on the layering principle and on the broad version of the end-to-end arguments.[9] As a consequence of that design, the Internet was application-blind i.e. it was unable to distinguish among the applications on the network, and as a result, it was unable to make distinctions among data packets based on this information. The Internet's application-blindness is one of the factors that have fostered innovation in the past and made the Internet more valuable for users and for society. It also contributed to the Internet's ability to improve democratic discourse, facilitate political organization and action, and create a decentralized environment for cultural and political interaction in which anybody can participate.

Today, technologies such as Deep Packet Inspection have removed the application-blindness of the network. They allow network providers to identify the applications and content on their networks and to control their execution.[10] Considerations such as preventing the transmission of unsolicited communications and blocking access to objectionable content must not form part of permissible traffic management practices, as these usually involve the use of Deep Packet Inspection techniques that grant access to the contents of data packets in addition to their headers. As access to the contents of data packets (which may carry sensitive personal information) takes place without the knowledge or consent of users, such practices constitute gross violations of the users' right to privacy. Therefore, Traffic Management should be used only for technical reasons to provide users a better experience by prioritizing some data packets to facilitate the Internet's best-effort data delivery process and there should not be any commercial consideration for this.

There is also a need for greater transparency in traffic management practices adopted by Indian ISPs, as non-transparency in this regard would not only make room for the discreet deployment of anti-competitive and impermissible traffic management techniques, but also deprive users of crucial information that would determine their choice of service provider. In the present scenario, ISPs are

9 David D. Clark, The Design Philosophy of DARPA Internet Protocols, COMPUTER COMM.REV., Aug 1988, p. 106

10 Network Based Application Recognition and Distributed Network-Based Application Recognition, CISCOSYS., http://www.cisco.com/c/en/us/td/docs/ios/12_2s/feature/guide/fsnbarad.pdf (last visited April 23, 2015).

under no obligations – regulatory or otherwise – to disclose details on the traffic management practices in active use. This stands in stark contrast to the prevalent practices in external jurisdictions, including the United States of America, where the Federal Communications Commission's Open Internet Order 2010 requires ISPs to "disclose the network management practices, performance characteristics, and terms and conditions of their broadband services"[11]; the United Kingdom, where prominent ISPs have signed up to a voluntary Code of Practice that requires each one to produce a comparable table of traffic management information called a Key Facts Indicator[12]; and Brazil, where the Marco Civil da Internet (Internet Bill of Rights) asks Brazilian ISPs to "provide transparent, clear and sufficiently descriptive advance-notice to users of the traffic management and mitigation measures adopted, including those related to network security".[13] Imposition of similar transparency obligations on Indian ISPs is necessary to prevent the deployment of unfair and anti-competitive traffic management techniques and to inform user-choice. The information provided to the consumers should be worded simply and not buried under reams of legal and technical jargon that are difficult to decipher.

Aside from the lack of transparency in traffic management, a number of previous content and service offerings by Indian ISPs and content providers have raised net neutrality concerns. This included the prevalent practice of zero-rating, both through dedicated platforms such as Facebook's Free Basics and Airtel Zero and through zero-rated access packs for particular websites such as Facebook and Twitter. While such practices have now been halted, thanks to TRAI's prohibition of differential data tariffs through its Regulation against differential pricing, service providers have been attempting to call the Regulations into question and circumvent its prohibition in creative ways including by claiming confusion regarding the permissibility of differentially priced content and services delivered over Closed Electronic Communications Networks. Multiple letters have reportedly been written to TRAI by ISPs and other industry consortia over the question of offering non-neutral services over CECNs despite the Regulations being amply clear on the fact that the use of CECNs to circumvent the prohibition on discriminatory tariffs will not be permitted. We wish to highlight these attempts at obfuscating the application of the Regulations as activities that raise concerns regarding potential net neutrality violations.

11 Federal Communications Commission, *Open Internet Order, 2010*, available at: https://www.gpo.gov/fdsys/pkg/FR-2011-09-23/html/2011-24259.htm, last accessed on July 2, 2016

12 OfCom, *Improving Traffic Management Transparency*, November 24, 2011, available at: http://consumers.ofcom.org.uk/news/improving-traffic-management-transparency/, last accessed on July 2, 2016

13 Article 9, Marco Civil da Internet, translation available at: https://www.apc.org/en/blog/marco-civil-brazilian-internet-bill-rights-english, last accessed on July 2, 2016

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

What we require are bright-line regulations on telecommunications service providers that would protect the principles of net neutrality and maintain its integrity by mandating the providers to not discriminate against any type of content and service. Any regulatory method and rules must preserve a "free and open" Internet that gives everyone in the country the same access to any website hosting legal content, including video, music, photos, social networks, email, and maps.

In October 2011, India made its stance on Internet Neutrality clear at the 66th session of the UN General assembly. India recognized that the Internet was an "unprecedented global medium" that should be "inclusive, democratic, participatory, multilateral and transparent in nature". India pointed out that the Internet had grown in size and scope, and the task of Internet governance required "quick footed and timely global solutions and policies, not divergent and fragmented national policies."[14] Subsequently, a Committee constituted by the Department of Telecommunications in May 2015 to enquire into the issue of net neutrality in India presented its findings in a 110 page report titled "Net Neutrality: DOT Committee Report".[15] The report observed among others that user rights on the Internet need to be ensured so that TSPs/ISPs do not restrict the ability of the user to send, receive, display, use, or post any legal content, applications, or services on the Internet, or restrict any kind of lawful Internet activity or use, and that the functioning of competitive markets in network, content and applications must be ensured by prohibiting and preventing practices that distort competition. Following this, the Prohibition of Discriminatory Tariffs in Data Services Regulations, 2016 were issued by TRAI in February 2016, which prevented TSPs/ISPs from offering and charging discriminatory tariffs on the basis of content, indirectly solidifying regulatory respect for the principle of net neutrality.

When nation's wealth, like spectrum, is being dealt with either by the Union, State or its instrumentalities or even the private parties, like service providers, they are accountable to the people and to the Parliament. This was held by the Supreme Court, while deciding the scope and ambit of powers of the Department of Telecommunications, TRAI and CAG in the case of *Association of Unified Tele-Service Providers & Ors. vs. Union of India*[16] where it was also ruled

14 Available at: http://www.itforchange.net/sites/default/files/ITfC/india_un_cirp_proposal_20111026.pdf

15 Department of Telecommunications, *Net Neutrality: DOT Committee Report*, May 2015, available at:http://www.dot.gov.in/sites/default/files/u10/Net_Neutrality_Committee_report%20(1).pdf, last accessed on July 2, 2016

16 (2014) 6 SC 110

that “State actions and actions of its agencies/instrumentalities/licensees must be for the public good to achieve the object for which it exists, the object being to serve public good by resorting to fair and reasonable methods. State is also bound to protect the resources for the enjoyment of general public rather than permit their use for purely commercial purposes. Public trust doctrine, it is well established, puts an implicit embargo on the right of the State to transfer public properties to private party if such transfer affects public interest. Further it mandates affirmative State action for effective management of natural resources and empowers the citizens to question ineffective management”.

Spectrum has been considered to be a natural resource by the Supreme Court of India in a number of cases. The courts have held time and again that spectrum belongs to people, and State, its instrumentalities or licensee, who deal with the same, hold it on behalf of the people and are accountable to the people. The State is therefore bound to act in consonance with the principles of equality and public trust and ensure that no action is taken which may be detrimental to public interest. This was held by the Supreme Court in *Centre for Public Interest Litigation v. Union of India & Ors.*,[17] where the issue for consideration before the court was whether the Government has the right to alienate, transfer or distribute natural resources/national assets otherwise than by following a fair and transparent method consistent with the fundamentals of the equality clause enshrined in the Constitution. In this case the court held that “When it comes to alienation of scarce natural resources like spectrum etc., it is the burden of State to ensure that a non-discriminatory method is adopted for distribution and alienation, which would necessarily result in protection of national/public interest”.

There are several ways to enforce the principles of Net Neutrality, including the following:

a) In exercise of its powers under Sections 11(1)(b)(v) and 36 of the TRAI Act, TRAI could issue a set of legally binding regulations that embody and thereby enforce the principles of net-neutrality, and the DOT could amend the license terms under which TSPs operate, mandating strict observance of said TRAI regulations.

b) Based on responses received to the consultation paper, TRAI could [in exercise of its powers under Section 11(1)(a) of the TRAI Act] make recommendations to the DOT concerning the incorporation of net-neutrality respecting obligations into TSPs' service licenses. Giving

17 (2012) 3 SCC 1

effect to the recommendations and incorporating relevant terms into service licenses would cement the TSPs' obligation to respect the principles of net-neutrality in their conduct.

c) In exercise of its powers under Section 11(1)(a) and based on the responses to the consultation paper, TRAI could make recommendations before the Central Government to enact a new central legislation or amend an existing legislation such as the Indian Telegraph Act in order to mandate strict adherence by TSPs to the principles of net-neutrality. Giving effect to these recommendations would again oblige TSPs to respect the principles of net-neutrality at all times.

Question 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.

The current legal framework for communications surveillance in India, surveillance of telephone networks is provisioned by Section 5(2) of the Indian Telegraph Act, 1885 read with Rule 419A of the Indian Telegraph Rules, 1951, while surveillance of Internet networks is provisioned by Sections 69 and 69B of the Information Technology Act, 2000 read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 as well as the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

These legislations collectively lay down the substantive and procedural frameworks under which Law Enforcement Agencies may collect communications data and meta-data from communications service providers. In the case of TSPs, their respective service licenses contain clauses that further outline certain security conditions in support of the broader legislative framework.

Setting aside the procedural laws and license clauses, even a perfunctory examination of Sections 69 and 69B of the IT Act will tell us that the Law Enforcement Agencies' surveillance powers under these Sections extend to “any information stored on a computer resource”, regardless of the characteristic attributes of said computer resource. Further, the Sections require any person/intermediary in charge of the computer resource to extend all surveillance-related assistance to Law Enforcement Agencies when called upon to do so, and failures in this regard are punishable with imprisonment for up to seven years and fines.

By virtue of the IT Act's broad definition of the term “computer”, literally any data that is

generated, stored or transmitted over any hardware (including servers, PCs, laptops, phones and tablets) or even software is capable of being surveilled by Law Enforcement Agencies, and the obligation to assist Law Enforcement Agencies in this regard accrues to all persons/intermediaries in charge of said hardware/software (including all OTTs, whose traffic traverses India).

On the question of compliance where the TSP or a content provider is based outside India, the Information Technology Act has broad territorial jurisdiction that extends to computer networks outside the country as well. Under Section 75 of the Act, this jurisdiction can apply to an offense or contravention (say that of sensitive data protection rules) as long as it involves a computer, computer system or computer network located in India.

Granted, there might be some difficulties in ensuring compliance by overseas players, but this is hardly endemic to India or its regulatory setup. The Internet, on account of its border-less nature routinely throws up jurisdictional challenges such as these, but it is important to bear in mind that regulatory efforts aimed at their redressal must not fundamentally alter the underlying principles of the Internet. Mutual Legal Assistance Treaties with specific provisions on the procurement of surveillance data from overseas communications service providers could be a more sustainable solution.

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

The Information Technology Act,2000 specifically encompasses laws relating to the cyber space i.e. electronic and digital signatures, data protection and privacy, and cyber crimes to name a few. With respect to maintenance of privacy, TSPs and content providers have to comply with Section 43A of the Information Technology Act, 2000 while handling sensitive personal data, along with adhering to the procedures laid down in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The above mentioned laws are applicable to a body corporate, which includes companies, firms, sole proprietorship, or even individuals engaged in providing commercial or professional services. The 2011 Rules on reasonable security practices enumerate the process for collecting, handling, and securing sensitive personal data of users, such as passwords, financial information, medical history, biometrics, etc. Moreover, the rules mandate an inclusion of a Terms of Service for all platforms engaged in collecting personal information about their users. Section 43A provides for a recourse to

the user when the data handler, in this case the TSP or the Content service provider has failed to adequately implement the security safeguards and has subsequently caused wrongful loss to the user or wrongful gain to another. In addition, the IT Act, 2000 provides for Section 72A, under which disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract is punishable with fine & imprisonment.

Specifically for TSPs that are also Internet Service Providers (ISPs), their license agreement with Department of Telecommunication (DoT) prohibits an encryption beyond 40 bits on their platform by users without prior approval of the DoT. For secure financial transactions, transmission of other sensitive personal data, and maintenance of privacy in general, it should be permissible to freely use encryption standards higher than 40 bits.

Both the TSPs and the Content Service Providers are intermediaries as per the Section 2(w) of the IT Act, 2000, and inevitably collect certain personal information about their users. Where protection and handling of sensitive personal data has been covered to a reasonable extent under the 2011 Rules; personal information (demographic information, email addresses, date of birth, and the like), along with meta data (location information, IP address, etc.) has not been accounted for substantially under the IT Act. These categories of information are the most widely collected, and shared amongst businesses, and internationally as well.

On a comparative note, the Federal Communications Commission (FCC) in the United States promulgated regulations for Protecting the privacy of customers of Broadband and other Telecommunication Services in March 2016, and sought comments from the public as well. These rules apply to Internet Service Providers (ISPs) and contain provisions that aim to provide customers the required tools to make informed decisions regarding their privacy while they are using internet services. A few significant provisions in this regulation is the three tier system of consent; notifications at the time of data breach; and prohibition on making services contingent to surrendering the privacy.

- Consent: This Regulation details a three tier system of consent to be followed by the ISP; first, where the customer provides the ISP with inherent consent to use their personal information to perform the essential service of sending information to its destination, or intimate about billing cycles; second, the customer has the option of 'opt-out' from permitting the ISP to use their personal information to market other communication related

services; and third, that the ISP will need specific explicit consent by the customer, i.e. an 'opt-in' for any other use of their personal information.[18]

- Data Breach Notification: In addition, this Regulation proposes a strict notification regime to the customer, as well as certain law enforcement agencies, in instance of a data breach, within a stipulated time frame of 10 and 7 days respectively. The law enforcement agencies are to be notified if the personal information of more than five thousand people is believed to have be breached.[19]
- Prohibition from making services contingent on a customer surrendering their privacy: This rule was put in place to ensure that in situations of less competition among ISPs, customers are not daunted by a 'take it or leave it' approach, where service providers make their services contingent to certain waiver of consumer's privacy.[20]

Although these regulations only cover ISPs and not Content Service Providers, these do serve as a point of reference for domestic regulators seeking to provide for adequate user privacy safeguards in the digital world.

Currently, the IT Act, 2000 although covers some ground with respect to data protection, the privacy and data protection regime in India requires an overarching law. In order to ensure that the personal information of users is protected, a foundational and comprehensive data protection law is required for India that can delineate the rights, and responsibilities of both users and data processors will provide the requisite guidelines for TSPs & CSPs for safeguarding the privacy and personal data of their customers. As the sectoral regulator for the telecommunications industry, and having conducted multiple public consultations that addressed the issue of user privacy in telecom services, TRAI would be well-placed to make a formal recommendation to the Indian legislature outlining the need for overarching privacy and data protection laws.

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

The issue over functioning of Closed Electronic Communication Networks (CECN) is one that has

18 Federal Communications Commission, *Protecting the Privacy of Customers of Broadband and other Telecommunications Services*, para. 107, available at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf, last accessed on July 5, 2016
19 Ibid., para. 236
20 Ibid., para 258

to be considered for a comprehensive policy framework for defining the relationship between TSPs & OTT content providers. In the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016, the proviso to Section 3(2) exempts data services provided over "closed electronic communications networks" (CECNs) from the general prohibition on differentially priced data services. While the proviso does make it clear that the prohibition would still apply if CECNs are leveraged in such a manner as to circumvent it, some industry players and consortia have been observed attempting to obfuscate this understanding by claiming a lack of clarity as regards the ambit and application of the proviso.

We wish to submit that the Regulations in general and the proviso to Section 3(2) in particular are both well-grounded in reason, and leave no room for ambiguities in their interpretation. As per the Regulations, differentially priced data services offered over the open Internet stand prohibited at all times, whereas such pricing arbitrages in internal CECNs that are separate and distinct from the open Internet will be allowed and will attract no financial disincentives from the regulator. Attempts at circumventing this regulatory premise are easily identifiable as such – offering content from particular content providers at discounted rates over a CECN to the subscriber base of a TSP for instance, is a clear circumvention of the prohibition on differential pricing.

That being said, we submit that it would nevertheless be beneficial in the interest of precluding further efforts at obfuscation and compromise to clearly outline the scope of exemption under Section 3(2) by way of illustrative examples of both permitted and prohibited uses of CECNs as a means of data delivery at differential tariffs.

We reiterate that TRAI is the apposite sectoral regulator for the telecommunications industry, and having already laid down a model Regulation against differentially priced data services, the focus going forward must be on ensuring its sound implementation rather than entertaining unfounded exhortations for its reconsideration.

Moreover, the earlier consultation on Regulatory Framework for Over-the-top (OTT) services overlaps with the current consultation process. Hence, it is important to have a definite road map and to have a time-bound plan to finalize the process. The comments and counter-comments provided in the earlier consultation on Regulatory Framework for Over-the-top (OTT) services will have to be considered with the present pre-consultation paper.