Consultation Paper on Regulation of OTT Services: Counter Comments

Following our initial comments on the Consultation Paper on Regulatory Framework for OTT Services, below are our set of counter comments that serve as responses to the comments made by TSPs and TSP associations. Though a number of substantive proposals have been made in response to the Consultation Paper, owing to the large volume of comments, we have identified some common themes found across the submissions made by major TSPs and TSP associations and presented our responses accordingly. The responses cover the following broad areas of discussion:

- Regulation of OTT service providers
- Security obligations on OTTs
- Net neutrality
- Zero-rated services
- Impact of OTT services on TSP revenues

Our general comments on these broad areas, as well as specific responses to comments by TSPs and TSP associations are given below.

Regulation of OTT service providers

A common theme that emerges from the submissions made in response to the Consultation Paper by most TSPs and TSP associations is the supposition that communication services provided by some OTTs are perfect substitutes for traditional communication services provided by TSPs. OTTs such as Skype, Viber and Whatsapp for instance, were highlighted as providing VoIP and Instant

Messaging services that are substitutable with the traditional voice/messaging services provided by TSPs. This being the case, it was said that a *Same Services, Same Rules* policy needs to be adopted in regulating OTT communication service providers, which means they need to be regulated under a framework identical to that regulating TSPs.

Several regulatory models were proposed in this regard, including:

- Bringing OTT communication service providers under the telecom licensing regime
- Classifying OTT communication service provides as Other Service Providers with some added security and revenue related obligations
- Imposing added regulatory obligations on OTTs other than through the licensing model
- Relaxing regulatory obligations on TSPs to bring them at par with OTTs

Without going into the merits and demerits of specific regulatory models, we wish to point out firstly, that a *Same Services, Same Rules* policy would result in inequitable regulation of OTTs as against TSPs for the simple reason that the communication services offered by each are not the same by any stretch of imagination. Similarity of communication services depends not only on the underlying function served, but also on the technical and architectural frameworks over which said services function.

To illustrate, OTT voice communication services such as those offered by Skype and Viber transmit communication data over IP networks (in this case, the Internet). Just like any other instance of information exchange over the Internet, this communication data is delivered in the form of data packets based on a best-effort delivery model, with no dedicated end-to-end channel being established for the duration of the communication. This stands in stark contrast to the traditional voice services offered by TSPs, which function atop circuit-switched PSTN architectures, where dedicated channels of communication are established between devices for the duration of the communications. OTTs such as Whatsapp and Hike similarly deliver their Instant Messaging data over existing IP networks as opposed to traditional SMS services, which utilize dedicated infrastructures involving Short Message Centers, Short Message Entities and SMS gateways among others. Communication services offered by OTTs and TSPs differ further in terms of functionality, in that the former's reliance on existing IP networks for content delivery enables them to bundle additional services such as multimedia file transfer, location based services and so on with their primary service offerings.

In light of the functional and architectural differences that exist between communication services provided by OTTs and TSPs, differential models of regulation for OTTs and TSPs become inevitable so as to preserve and allow the continued development of said architectures. Efforts at introducing additional regulatory frameworks aimed at leveling the regulatory playing field with respect to fundamentally different business entities would prove to be counter-productive and serve only to stifle innovation and healthy competition in a free market environment.

Moreover, as we had stated in our comments to the Consultation Paper, OTT communication service providers are already regulated by a number of general and specific legislations that prescribe numerous general, technical, financial, and security related conditions that OTTs must necessarily comply with. Some of the existing legislations that apply to OTTs are:

- Information Technology Act, 2000
- Consumer Protection Act, 1986
- Payment and Settlement Systems Act, 2007
- Indian Copyright Act, 1957

- Income Tax Act, 1961
- Customs Act, 1962
- Central Excise Act, 1944
- Foreign Exchange Managements Act, 1999
- Prevention of Money Laundering Act, 2002

As OTTs are already regulated under the above legislations, we submit that additional regulatory frameworks would be excessive and would hinder the growth of the OTT service industry. We feel the purpose of ensuring comprehensive regulation of OTTs would be better served by a review of how the existing regulations apply to OTTs and making necessary amendments based on the findings, rather than establishing a dedicated regulatory framework from scratch. Regulations and laws prevailing over telecommunication services such as entry fees, spectrum allocation and charges, tariff regulations etc. cannot be imposed on OTT services for the reason that regulation of websites and apps provided on the Internet would have a direct impact on start-up companies and new entrants who will be forced to comply with regulatory costs notwithstanding the cost of setting up the website in the first place which is very low or even negligible. The Internet provides an opportunity to everyone, be it college students who are constantly coming up with great, innovative business ideas and even people in rural areas who are able to sell their products on the internet. Over-regulation would mean a loss of all such opportunities and a sudden hindrance to innovation.

Security obligations on OTT service providers

The fact that OTTs bypass all national security and surveillance related obligations imposed by law on TSPs was highlighted in the Consultation Paper as a major regulatory drawback that needs to be rectified. This was echoed by almost all major TSPs and TSP associations in their comments, and was said to contribute to a regulatory imbalance as far as TSPs and OTTs are concerned. While TSPs are under strict legal mandates to make room for the surveillance of all information that flows over their networks, it was said that OTTs bear no such obligations, making it impossible for LEAs to monitor India's OTT traffic in the interest of national security.

To quickly recap the 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 LEAs 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 LEAs' 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 LEAs 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 LEAs, and the obligation to assist LEAs in this regard accrues to all persons/intermediaries in charge of said hardware/software (including all OTTs, whose traffic traverses India).

This being the case, it is fallacious to state that OTTs bypass all national security and surveillance related obligations mandated under law, since these obligations are clearly as applicable to OTTs as they are to TSPs. Granted, there might be some difficulties in ensuring compliance by overseas OTTs, 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.

On a related note, a few TSPs in their comments to the Consultation Paper, have depicted the high levels of encryption used by some OTTs as undermining Indian LEAs' surveillance capabilities. It has been suggested for instance, that since LEAs often request TSPs to provide encrypted OTT communication data whose decryption keys are naturally not available with the TSPs, it is essential in the interest of national security that encryption be permitted only where it is indispensable for user safety and privacy. Another radical solution was highlighted in requiring OTTs to deposit their decryption keys with surveillance systems such as the Central Monitoring System so as to facilitate real-time surveillance by LEAs.

Proposals such as these come with staggering implications on user privacy. The right to privacy is a jurisprudentially recognized fundamental human right both domestically as well as internationally. To prohibit encryption of communication data except when absolutely necessary would be a brazen violation of this right, and to have OTTs deposit decryption keys with LEAs would defeat the very purpose of encryption, leaving users' communication data vulnerable to unauthorized access.

Moreover, high levels of encryption won't ever be an impediment to legitimate surveillance if LEAs make their data requests to the concerned OTTs themselves, as opposed to TSPs that merely carry the encrypted traffic.

Net neutrality

In view of the substantial liberties some TSPs and TSP associations have taken in understanding the term “net neutrality”, we express our strong reservations against altering the established concept of net neutrality to suit individual preferences. The argument for net neutrality 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.[1] 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.[2] This innovation theory is embodied in the end-to-end network design argument, which in essence suggests that networks should be neutral as among applications.[3] 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.[4] The very fact that the Internet is the fastest growing network in history is evidence of the superiority as well as indispensability of this principle.

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, and any understanding of net neutrality that attempts to shift focus from this fact must be seen as subversive. One such interpretation of net neutrality,

[1] 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

[2] Ibid.

[3] J H Saltzer et al., *End-to-End Arguments in System Design*, available at: http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf

[4] Supra.

which a number of TSPs have embodied in their comments to the Consultation Paper, portrays equal access to the Internet as the driving force behind calls for net neutrality, allowing for the introduction of developmental paradigms that seemingly prioritize access above all else. While it is true that access is an important consideration in a developing nation such as India, where around 80% of the population still lacks basic access to the Internet, we believe that service arrangements aimed at proliferating access must not be to the detriment of the Internet itself.

We believe that a truly neutral Internet should necessarily be guided by the following principles:

1. No application-based discrimination: The Internet must be neutral as amongst applications. There must be no discrimination of data packets based on content, applications, services, or classes of applications or services.
2. No paid prioritization: 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/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.

Departure from these principles must be allowed only to give effect to legislative provisions or court orders. Traffic Management could 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. 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. Bharti Airtel for instance, had submitted in their comments to the Consultation Paper that traffic management allows them to protect users from spam and to restrict access to age-inappropriate content. Filtering spam and objectionable content would necessarily require access to the contents of data transmissions, pointing to the possible use of DPI to meet this end. DPI techniques must be prohibited across the board other than for legitimate reasons specified under law. Another benefit of traffic management as pointed out by Bharti Airtel was its ability to enable the provision of premium services to enterprise customers to meet their business needs. Provision of premium services does not fall within the scope of traffic management and runs foul of the principles of net neutrality by prioritizing applications. Practices such as these should therefore be disallowed as being violative of net neutrality.

In addition to prioritizing data only in the interest of traffic management and giving effect to legislations/court orders, TSPs must be also transparent about their traffic management and network administration practices. Users must be provided transparent, clear and sufficiently descriptive information about such measures. The six principles put forward by OfCom i.e. appropriate, accessible, understandable, verifiable, comparable and current may be adopted as transparency standards.

Zero rated services

One of the most consistent arguments put forth in favor of zero rated services is that they are necessary for consumer digital inclusion. It is argued that services need to be made affordable enough for large scale adoption and pricing innovations such as zero rating act as catalysts in achieving this goal.

The practice of zero rating makes certain kinds of traffic exempt from any data cap at all, or creates a synthetic "online" experience for users that isn't the Internet. Traffic that is "approved" is allowed; other traffic won't flow to users. This practice is discrimination on the basis of traffic itself, being carried out by the service provider – not by the user.[5] Thus, Zero-rating could result in the emergence of haves and have-nots, where inequality is entrenched in differential access to services based upon data and instead of a purely digital divide, there will be a data divide.[6]

A better approach for closing the digital divide is the adoption of policies that drive towards openness and competition – steps like requiring carriers to offer dark fiber services (unused capacity that retail providers can use to send information) that can be used by competitors as essential infrastructure. Digital literacy for non-adopters plus heightened awareness of how the Internet is relevant to their lives are needed as well.[7] If ISPs want to help undeserved communities there are better options that are entirely compatible with meaningful network neutrality rules. Plans that offer "free," unlimited use of applications are based on calculations about the average amount of data users use for this application. Rather than giving away bandwidth that can only be used for specific websites/applications, wireless providers could give away a comparable amount of bandwidth that can be used to access the full Internet. These minimal plans would cost the providers the same as zero-rating. Alternatively, providers could offer subsidized plans that are only available to low-income customers. For example, most German providers offer mobile data plans for students that include more monthly data than regular plans at lower costs. These alternatives would come at no extra cost to providers, but they would provide enormous benefit to low-income communities.[8]

The Regulator should consider alternate approaches that include partnerships between TSPs and OTT Players, which could serve as solutions to the challenges that zero rating seeks to address. Eg. Mozilla has sought to create such an alternative in its Firefox OS ecosystem. In Bangladesh,

[5] *Zero for Conduct* by *Susan Crawford available* at https://medium.com/backchannel/less-than-zero-199bcb05a868

[6] http://www.techrepublic.com/article/zero-rating-poses-a-conundrum-for-net-neutrality-advocates-around-the-world/

[7] *Ibid.*

[8] Network Neutrality and Zero-rating, Barbara van Schewick, February 19, 2014 available at http://apps.fcc.gov/ecfs/document/view?id=60001031582

Mozilla(in partnership with Telenor) allows users to receive 20 MB of data usage for free each day, in exchange for viewing an advertisement. In Africa, consumers can buy $40 Firefox OS smart-phones(in partnership with Orange) that come packaged with 6 months of free voice, text, and up to 500 MB per month of data. According to Mozilla, scaling up arrangements like these could represent a long-term solution to the key underlying problems of digital inclusion and equality.[9]

Zero rating distorts competition, harms start-up innovations, small businesses

Fees in exchange for zero-rating poses the same threat to innovation and free speech as fees in exchange for preferential treatment. Start-ups, small businesses and low cost speakers will often be unable to pay to be in the fast lane; they won't be able to pay for zero rating, either. These companies will not have a chance to be heard and compete with those companies that can pay so that their content loads faster or does not count against users' bandwidth cap.[10] If zero rating is not explicitly outlawed, we hand immense power to TSPs/ISPs. In effect, they can become gatekeepers – able to handpick winners and losers in the market. Thus the contentions of certain TSPs that if structured properly, zero rating can result in increased competition seem unfounded.

Impact on first time zero rated service users

Claims by TSPs that there is little evidence to show that free access to content, which is what zero rating provides to consumers, will somehow lead to diminished online freedom and innovation is baseless. In fact various studies carried out in countries where zero rated services have been introduced, have observed a misconception among users, eg. A 2012 study carried out by LIRNEasia in Indonesia shows that masses of Facebook Zero users replied in negative to questions of internet use. It observes *"It seemed that in their minds, the internet did not exist; only Facebook"*[11] Another survey on communications use in Africa showed that the number of people

[9] https://blog.mozilla.org/netpolicy/2015/05/05/mozilla-view-on-zero-rating/
[10] Supra 4
[11] http://lirneasia.net/2012/05/facebook-internet/

who had responded saying they used Facebook was much higher than those who said they used the Internet. A more recent survey conducted by *Quartz* in Indonesia and Nigeria shows that at least a few millions of Facebook's 1.4 billion users suffer from the same misconceptions.[12] The survey observes that in both countries more than half of those who don't know they're using the Internet say they "never" follow links out of Facebook, compared with a quarter or less of respondents who say they use Facebook and the Internet. If people stay on one service, it follows that content, advertisers, and associated services also will flow to that service, possible to the exclusion of other venues.[13]

Zero rating harms consumers

If TSPs can charge OTTs to be zero-rated, they would have an incentive to lower monthly bandwidth caps or increase the per-byte price for unrestricted Internet use in order to make it more attractive for applications providers to pay for zero-rating. The resulting reduction in bandwidth caps harms users and providers of applications that do not pay for exclusion from the cap. Research shows[14] that in November 2014, in many OECD markets, where mobile operators launched zero-rate film stores and TV services, consumers are either not allowed to buy more than a few (5-10) gigabyte at all or most likely, they cannot afford to buy more because the price of additional gigabyte is prohibitively expensive. Consumers are harmed because their choice of Internet video service is severely restricted.

By contrast, shortly after the Dutch regulator prohibited ISPs from zero-rating their own applications, KPN doubled its monthly bandwidth cap for mobile Internet access from 5 to 10 GB at no additional cost. It was about to introduce its own mobile TV application, and had planned to zero-rate it. But with zero-rating off the table, KPN faced a choice of offering an application that

[12] http://www.theatlantic.com/technology/archive/2015/02/facebook-is-bigger-than-the-internet-whoa/385350/

[13] http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/

[14] http://www.dfmonitor.eu/downloads/Neelie_Kroes_Specialized_Services_are_a_giant_net_neutrality_loophole_HIGHLIGHTS.pdf

users can’t use (because the bandwidth caps were too low), or increase the bandwidth cap so that users can actually use KPN’s application - but in a way that allows users to choose freely among competing applications. Thus, banning zero-rating ultimately benefits all users (even those that aren’t interested in using the zero-rated application) and all applications, by making more unrestricted bandwidth available.

Zero-rating is a powerful tool to favor some applications over others and causes the same problems as technical forms of differential treatment. Like technical forms of discrimination, zero rating may be used in one of three ways:

- An ISP can offer applications providers to pay for zero-rating
- An ISP can zero-rate selected applications in a class of similar applications without charging the providers of zero-rated applications
- An ISP can zero-rate all applications in a class without charging the providers of the zero-rate applications

Like the different kinds of technical discrimination, these different kinds of zero-rating pose different problems, and should be evaluated separately.[15]

Revenue impact of OTT services

Another common theme that emerged from the submissions made by TSPs and TSP associations is the contention that the proliferation of OTT services has been greatly detrimental to revenues from traditional voice/messaging services. Several sets of statistics were provided evidencing this decline in traditional revenue. However, what these submissions fail to demonstrate clearly is whether said decline in traditional revenue is offset by the corresponding spike in mobile data revenue. As the Internet penetrates ever deeper into citizens' everyday lives, the volume of data that is exchanged as

[15] Supra. 4

result has also risen exponentially, leading to a commensurate growth in money spent in terms of data charges. In most cases, this rise in mobile data revenue has far outpaced any fall in traditional revenue that it may have caused.

As submitted in our response to the consultation paper, while the Average Revenue Per User (ARPU) for Voice has remained steady and has gone up from Rs. 154 to Rs. 157 in the 3rd Quarter of 2014 - 2015, the ARPU for Data has increased substantially in the last three years, from Rs. 40 to Rs. 170 for Airtel, Rs. 47 to Rs. 126 for Idea. Mobile traffic has also seen a substantial increase from 7,175 Mn. Mbs to 46.077 Mn. Mbs for Idea, 17,400 to 65,778 for Reliance and 23,933.80 to 26,748.50 for Airtel. Besides, Airtel in a management presentation dated November 2014[16], itself stated that India is expected to have one of the fastest growth rates in the data segment over the next 5 years, to be driven by low cost mobile handsets and new technologies (3G/4G). Data revenues for Airtel are expected to go to 32% for India as a % of total revenue.

Therefore, the argument that TSPs are losing out because of increased use of data is untrue. Evidence collated from TRAI shows the following developments between June 2013 to September 2014[17]:

- ARPUs have gone up from 111 to 116, a Rs. 5 increase. (per month)
- Of that, Call Revenue per user is down by Rs. 3.18 per user per month, and SMS revenues have fallen by 24 paise per month.
- Data revenues are up by Rs. 10.46 per month per user

In any business, the product matrix and the contribution from each product or service will change

[16] Slide 15 of 34, available at http://www.airtel.in/wps/wcm/connect/0cddd6cf-eaac-42e5-8366-da7cf62f087d/Bharti-Airtel_Management-Presentation-Q2FY15.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=0cddd6cf-eaac-42e5-8366-da7cf62f087d

[17] Data available at http://capitalmind.in/2015/04/telecom-companies-are-not-losing-money-to-data-services-the-net-neutrality-debate/

over a period of time depending on various factors like technology and customer preferences. The sectoral regulator does not have any role in this market driven scenario. Moreover, this exponential rise in mobile data revenue in the face of declining traditional revenues is a global phenomenon, and is not restricted to India by any means. TSPs world over have adapted to this change in several ways, including by entering the OTT service industry themselves. In other words, it is essential that TSPs adapt to changing technologies and not stand in the way of innovation due to an unwillingness to forgo revenue from traditional voice/messaging/VAS sources.