Date: 24th April 2015

Ref: OBSINPL/TRAI/FY15-16/006

To,
Shri A. Robert J. Ravi
Advisor (TD &QoS)
Telecom Regulatory Authority of India
Mahanagar Door Sanchar Bhawan,
Jawahar Lal Nehru Marg, New Delhi – 110 002

Subject: Response to TRAI's Consultation Paper No.02/2015 dated March 27, 2015 on Regulatory Framework for Over-the-Top (OTT) Services

Dear Sir,

We are pleased to enclose our thoughts and suggestions on the captioned Consultation Paper.

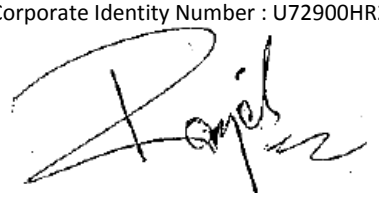
A brief background on Orange Business Services: -

Orange Business Services, is one of the world's leading telecommunications carriers (telecom service provider and telecoms network operator) with customers in 220 plus countries and territories. Orange Business Service India provide enterprise services to multi-sited corporations, Indian BPO outsourcing and ITES sector operating global networks and holds NLD, ILD & ISP license issued by Department of Telecommunications.

Please find enclosed our views in the enclosed annexure and we shall be glad to provide any clarifications and further details on our thoughts and hope our views would be useful in arriving at meaningful conclusions.

Thanking you,
Yours sincerely,

For Orange Business Services India Network Pvt. Ltd.
Corporate Identity Number : U72900HR2007PTC037029



Rajesh Ballal
Compliance & Regulatory Head (South Asia)

Orange Business Services (hereinafter 'Orange') response to TRAI's consultation paper on 'Regulatory framework for over –the-top (OTT) services and Internet Neutrality, dated 27th, March 2015.

Brief Introduction

At the outset, Orange welcomes TRAI's consultation paper on over – the - top (OTT) services and net neutrality.

The technical nature of services delivered over communication networks is rarely apparent from a user's point of view. Whether an application or service comes from a telecoms company or a pure OTT provider should neither be obvious nor of much interest, so long as the consumer gets what he or she expects. However, 'behind the screen', the differences are significant - both in terms of the rules under which they are governed and the confidence which the public may reasonably have in them.

Such a divergence is harmful to the immediate interests of consumers and to the longer-term health of our digital industries. For a clearer and indeed safer environment, out-of-date regulations should be removed or remodeled into a modern framework, creating a simpler, fairer marketplace where rules apply to all players and relate to the nature of a service - and not the means by which it is provided.

While telecommunications services developed long ago, the past two decades have seen an internet revolution transform citizens' lives and support the development of a wide range of new services, some of which partly replaced those for which the networks were originally conceived.

This growing range of innovation and uses opened up by the World Wide Web has been of a great benefit for consumers: the internet has become a huge

part of everyday lives. Completing transactions online has become second nature, with more and more people going online for shopping, banking, information and entertainment, a trend that will continue to increase with new services in the cloud for instance. This market evolution is definitely good for users choice, however, it also demands a fresh look at the regulation of digital services in order to ensure that similar services are governed in a similar way.

1. Comments on OTT

The current regulatory framework is not suited to these developments, leaving consumers often unprotected

Liberalization of the industry in the 90's brought in its wake many new policies aimed at protecting consumers. For the consumer specifically these included: access to emergency calls; simpler number portability rules; privacy and confidentiality obligations. On the public interest side, there were interoperability requirements; provisions on legal interceptions; personal data protection and many financial contributions.

Yet these policies were designed at a time when internet was still in its infancy. They therefore do not cover services provided by pure OTT players. This leads to a very complex situation that can be detrimental to consumers, public authorities and, last but not least, the development of fair competition between industry players. For example, customers are not protected the same way when they use internet-based services:

i. their location can be used without the same protection;
ii. they cannot access emergency services;
iii. when using a VoIP or messaging services from OTTs they are not under privacy or security rules, like the ones applying to telecoms services;
iv. law enforcers and regulators have no legal basis for intervention as legal provisions apply only to telecoms operators.

v. they do not have data portability rights when switching providers;

Some customers may neither be aware nor concerned about this situation, while others accept it for the sake of seemingly 'free' services - albeit at the cost of a lower level of privacy and security.

The Telecom Operators network simply carries the IP packets from source to destination. In this background it is necessary that there should be a regulatory framework which may ensure the following regulatory principles:

- Level Playing Field
- Security
- Privacy
- Transparency
- Quality of Service (QoS)
- National Government Policies

a common framework for digital services based on the principle: "same services, same rules"

All digital services should be governed the same way. This calls for a new regulatory architecture addressing all digital services, independently of the provider. Digital services are currently subject to distinct rules depending on the legal categories they belong to: electronic communication services (ECS – covering operators' services) or information society services (covering most internet services). With the internet revolution, those categories have now become obsolete as regards their technical or economic specifications. the current definition, information society services are services that are paid for, a characteristic which does not fit with the majority of internet services, often provided for free these days.

implementing common rules on digital services requires a multifaceted action plan

The current consultation debates focuses on how to defend an open internet from the network side while preserving its smart functioning and innovation. However, to ensure consistent protection, neutrality should not stop with networks and should apply to all internet players. Openness and transparency are required over the entire 'value-chain' - app stores, smart phones or tablets, as well as browsers and operating systems, not to mention search engines.

When establishing a common framework for digital services, the recommendations from the Authority should encompass provisions on internet neutrality such as transparency; openness (or non-blocking so customers can reach legal content and applications); interoperability and switching.

Report on internet platform neutrality

The French "National Digital Council" published in May 2014 a report highlighting that today, large platforms are the internet gatekeepers. As a consequence, the council has drawn up "recommendations deemed as priority areas to ensure that the upholding of the principle of neutrality by and within platform ecosystems"

http://www.cnnumerique.fr/wp-content/uploads/2014/06/PlatformNeutrality_VA.pdf

data protection for all services and users

A high and consistent level of data protection would mean that all citizens using internet services - email, payment or cloud services for example – could enjoy the same level of protection across all players offering services. Moreover, protection should be consistent regardless of the company involved (telecoms, OTT), or the technology. In short, here again, the same services should follow the same rules, no matter where, how or by whom they are provided.

Thus, we suggest a new framework should be implemented which is light touch regulation which encourages innovation, with strong protection for consumers and ensures that there is a level playing field in relation to similar services.

2. Comments on Net Neutrality

Internet has transformed the way people communicate, work and live by enabling a growing range of new services; more and more people go online for shopping, banking, information and entertainment, a trend that will continue to increase with the internet-of-things. It has opened up great opportunities in education, culture, communication, social interaction, as well as enabling advancements in science and technology and more broadly encouraging freedom of expression and media plurality.

Preserving the openness of internet, in the sense everybody should be entitled to distribute and access the content, services, apps of his/her choice, is therefore essential. This relates to network neutrality but also to the internet openness in its entirety.

internet success relies on efficiently managed networks

The constant growth in the use of the internet creates a challenge for network operators in order to meet demand. They do so by investing in new capacities and by managing existing capacity.

The internet needs continuous networks upgrades.

The internet owes much of its success to the wide availability of broadband. However, the tremendous increase of traffic, especially with growing video services, pushes for ever higher demand in terms of speeds and capacity in networks. To cope with this, operators continuously invest in new capacities, despite a difficult environment and shrinking revenues.

networks require traffic management to work properly and deliver the best experience to end users.

Even if network upgrades could meet the continuous need for greater capacity, it is inevitably rapidly exploited by new services – jump from TV to UHD TV for example. Consequently the need for operational support called 'traffic management' will never go away. Investments in increased capacity and traffic management are complementary tools to ensure the best possible customer experience.

Traffic management is necessary for operators to operate their network on a permanent basis (e.g. to orient traffic depending notably on the current performances of different routes), to prevent congestion, to effectively protect the security and integrity of networks, to restrict the transmission of unsolicited communication to consumers (e.g. spam) or to give effect to a licensing provision or court order (e.g. child protection).

The net neutrality requirements have traditionally been applied only to telecoms operators; but other providers in the internet value chain such as content delivery networks, browsers and proxies can also differentiate in terms of quality and service. A service like voice, video-streaming, etc., will have to be given priority over services such as email or messaging in order to ensure the best overall quality for all. Video services may be optimized, by compressing data, adapting content for mobile screens and reducing the cost to the consumer.

end users can have various types of services over a single access network.

An efficiently managed single access network allows the smooth co-existence of:

1. access to the internet content, application or services, provided over IP protocol, with no guarantee in terms of quality, also often named "best effort".

The network and the services are both agnostic and there is no “built-in” guarantee that data is delivered or that a user is given a guaranteed quality of service or a certain priority. Users obtain unspecified variable bit rate and delivery time, depending on the current traffic load. This is somehow similar to postal services; a sender usually cannot be certain that a letter was delivered or how long it will take. As highlighted by BEREC (Dec. 2012 - summary positions on net neutrality), this specificity is a driver for innovation, in the sense that innovative services can be developed without taking into account network constraints.

2. other services with a guaranteed quality – often named managed or specialized services.

This category encompasses conventional services such as IPTV, video on demand, future mobile voice over 4G, virtual private networks for business customers but also innovative services such as remote care or secure home solutions. They are characterized by specific requirements in terms of performance (e.g. time sensitive service), interoperability or reliability. With all services moving to IP-only networks, operators have to ensure that these characteristics remain guaranteed, calling for traffic management.

Co-existence of these two categories of services in a single access network is beneficial to all:

– the demand for specialized services calls for investments in new capacity, which in fine is also advantageous for internet access services;

– running specialized services requires a more efficient utilization of networks, minimising traffic loads on networks and improving the quality of the internet access over the same infrastructure;

– a dynamic allocation of capacity between the two categories of services improves the overall customer experience; on the contrary, imposing a

dedicated fixed capacity to some services would freeze such capacity even when these services would not be used by the customer; for instance, when IPTV is switched off, its capacity would not be available for internet access services.

best tools to guarantee network neutrality

The debate over net neutrality has mainly focused on operators using traffic management in a way which could be anti-competitive or hindering innovation, and on the impact of specialized services on internet access services. Considering the importance of the internet today, these concerns are comprehensible, even though there is little record of this happening. In any case, as the customers have already benefits from relevant safeguards via Regulatory intervention (as and when required), CCI etc.

As in the case in Europe, where network neutrality is already governed by competition and legislative provisions

Competition combined with transparency and switching rules imposed on operators are the best safeguards for network neutrality, as already highlighted by BEREC. In the European Union, broadband markets are characterised by strong competition and any degradation of services can lead to immediate consumers' reactions; "voting with their feet" they can switch providers, not to mention for the operators the negative impact on brand and revenues. Moreover, the fact that services over the internet have developed very successfully in Europe, even when they were competing with similar services offered by the operators, also suggests that concerns of anticompetitive behavior from operators' side are overstated.

In addition in Europe, the electronic communications framework already includes relevant rules on net neutrality. They give regulators a clear objective to safeguard net neutrality and empower them to adopt rules to preserve a minimum quality of services. They also impose operators to comply

with transparency measures. Many regulators have either adopted specific measures, like in France, or monitored the development of self-regulatory measures like in the UK.

any new initiative should be proportionate, simple and future proof, and be consistent.

To avoid a patchwork of national legislations and ensure harmonisation, any new measure should be taken by the Authority. In addition, in the fast moving environment of digital technologies, regulating network neutrality requires to avoid three major risks: adopting rules that would become quickly obsolete, that would pick the winner and/or second guess innovation, which should be for the market to decide.

To tackle these constraints, the best way forward appears to adopt a set of high level principles preserving network neutrality while allowing operators to efficiently operate their network and to innovate on services. Any regulation should focus on the outcomes, rather than to over-specify technical inputs.

While traffic management practices could be framed by principles such as transparency, proportionality or non-discrimination, it is equally important to acknowledge the necessity of those practices for a smooth network functioning. Finally, even if it may be appealing to call for all bits of traffic to be equal, this “equality” is not compatible with the way networks function. Traffic is indeed oriented diversely by routers, their function being precisely to route packets differently (i.e. not equally) depending on packets characteristics (first of all their destination) and information received on network availability or congestion. Interpreted too literally, a strict principle of net neutrality would conflict with the goals of network operation, lowering efficiency, security, and increasing congestion.

According to the AD Little study – the Future of the Internet – May 2014 "access networks experienced significant imbalances (in the order of 5 to 1) on average between incoming and outgoing traffic just because the nature of traffic today is media related and streaming, and therefore mainly flows one way from content providers to end users."

http://www.adlittle.com/downloads/tx_adlreports/ADL_LibertyGlobal_2014_FutureOfTheInternet.pdf

guaranteeing internet openness requires looking beyond network neutrality

For protection to be consistent, neutrality should not be limited to networks and should also apply to all players of the internet. Openness and transparency are required over the entire value chain - app stores, smart phones or tablets, as well as browsers and operating systems - not to mention search engines.

Only a holistic approach of the entire internet value chain could guarantee an open internet, which the Commission has still to initiate in the context of a thorough review of the regulation applied to digital services.

****