From: knath21@yahoo.in
To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>
Cc: "Joint Advisor CA" <jaca@trai.gov.in>, "श्याम सुंदर चांडक - Shyam Sunder Chandak, Advisor (RO-Jaipur)" <adv.jaipur@trai.gov.in>, traijaipur@gmail.com
Sent: Thursday, August 24, 2023 7:06:16 PM
Subject: Comments of the Consultation Paper on " Regulatory Mechanism for Over-The-Top (OTT) Communication Service and Selective Banning of OTT Services."

CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT

Hon. Sir,

Namaskar.

Please find herewith our comments on the Consultation Paper on " Regulatory Mechanism for Over-The-Top (OTT) Communication Service and Selective Banning of OTT Services."

You are requested to do needful and oblige.

Yours faithfully,

(Dr. Kashyapnath)
President
Member Organization : TRAI

Encl. : Comments.

CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT

Comments
On

Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services

Introduction :

India is one of the largest emerging markets for OTT video streaming services. In 2018, the Asia-Pacific region saw the steepest growth, of 24%, in the OTT video market globally. India has also seen in recent years a sustained debate about content regulation on OTT platforms. India has a vibrant audiovisual

industry. The overall media consumption in the country has been growing at an annual rate of more than 9% over the course of the last six years, one of the highest in the world. Digital media consumption has been also growing fast as the number of broadband users increased to more than 480 million. The number of internet users in India rose by more than 13.9%. People in India consume more than 190 minutes of video content a day on different platforms. The rate of consumption of video content has grown by 8% in the last seven years. There has also been an increase in platforms available for viewing, including OTT services and apps on different devices, apart from existing television channels. Regulating of OTT is emerging area to control and bring them into the preview of proper regulator control in India is very much essential in the present rapid growing technology.

The rapid growth of OTT services has raised a number of national policy issues relating to regulatory imbalances &

security concerns that need to be addressed. The regulatory imbalances need examination at various levels by different agencies of Government. In addition, public safety and privacy issues require attention.

A rapid ascension into a culture of 'binge-watching' has begun to phase out the days of Doordarshan and satellite disks, with OTT content offering leisure viewing at home. India's OTT viewership stands at 43 million people and is projected to rise up to 50 million by the end of 2023. The rising popularity of OTT platforms hosting a wide variety of content has often raised issues regarding its regulations.

Technological innovation enables the development of products and services that were simply not possible in the past. The combination of smartphones with their sophisticated operating systems and touchscreens and the widespread availability of relatively fast mobile broadband has enabled a broad range of applications and services to be provided. Some

of these such as WhatsApp and Fac eTimeare close substitutes for traditional voice and text messaging provided by operators. Other services such as Facebook, Instagram and Twitter offer not only communications but also a range of publishing and social networking services that were not feasible in the pre-smartphone era.

From the general perspective of innovation, it is not surprising that a set of innovative software development companies have emerged that are able to provide better customer experiences than the operators can provide. Increasing specialization is an intrinsic part of general economic development. In effect, while providers of OTT services increasingly specialize in and dominate the consumer experience, the traditional operators are being forced into a specialist commodity mobile broadband provider role. This type of industry disruption inevitably shifts the landscape that regulatory settings have been predicated on. There is almost no

aspect of regulatory intervention in telecommunications that is left untouched by this industrial transformation.

Given the complexity and scope of the regulatory responses required, it is useful to conceptualize these adaptations has been responses to a transition. This transition begins in the traditional circuit switched world and ends in the 'IP everywhere' world, although ongoing technological innovation will, no doubt, require further regulatory responses in the future. Many of the problems confronting regulators emerge because this transition is, as yet, incomplete but it is, nonetheless, within sight. The endpoint of this transition process would appear to be one in which mobile operators become pure mobile broadband providers. This does not necessarily mean that their services will have become completely commodified. There will still be opportunities for differentiation in their consumer facing activities across a range of characteristics including reliability, speed, congestion and

contention, customer service, and pricing. To the extent that, in the past, the full cost of data provision has not been reflected in the prices charged to consumers because of cross-subsidization from premium services, one of the adjustments required may be in terms of an adjustment of consumers' expectations about pricing of data services. In order for consumers' long-term interests to be served it is necessary that operators make sufficient margins to allow them to invest in upgrading infrastructure. To the extent that data services are underpriced currently, OTT providers are benefiting via cheaper consumer access to their services Over-The-Top Services: Understanding the Challenges and Opportunities that are being, to some extent, subsidized by operators through reduced margins. The sustainability of the situation is a central concern for regulatory evolution.

OTT or similar regulations were common in the European Union as well as in Australia, Britain, Indonesia, Vietnam and

Pakistan.

We feel that OTT rules should not be seen as a censorship effort, adding that it was more like a regulatory exercise to weed out toxic content such as pornography, bomb-making tutorials and other undesirable content on various digital platforms.

In that context, the upcoming regulation had nothing to do with a potential impact on people's freedom of expression and speech as some critics had said since only broadcasters, not individuals, would be affected.

We are in view that Regulatory measures should be aimed at protecting consumers since online content was accessible by all age groups. The TRAI should strike a balance to avoid hindering creative and innovative content while ensuring that there was a level playing field for all competitors. A right balance in the regulatory approach would lead to a reasonable tax-revenue base while undesirable content would be

minimized and businesses could prosper from new business models on the digital platform.

Any form of regulation should aim at the public benefit and protection of the public from potentially harmful effects. OTT regulations are intended ensure that “appropriate content” is distributed, meaning that it would have the proper copyrights and be appropriate for the audience in a given country. Some are concerned about operators distributing content without a copyright, so OTT services could be a key means to combat piracy.

One should also see that OTT regulations should not hinder the digital TV industry, which has been growing at a high rate. Politically sensitive content could also be affected by OTT regulations.

Repeatedly shutdown of telecommunications or the Internet can have significant ramifications for a country’s economy. It also disrupts critical services such as education and

healthcare. Consequently, such a shutdown affects the life and livelihood of the citizens of the country.

ISSUES FOR CONSULTATION

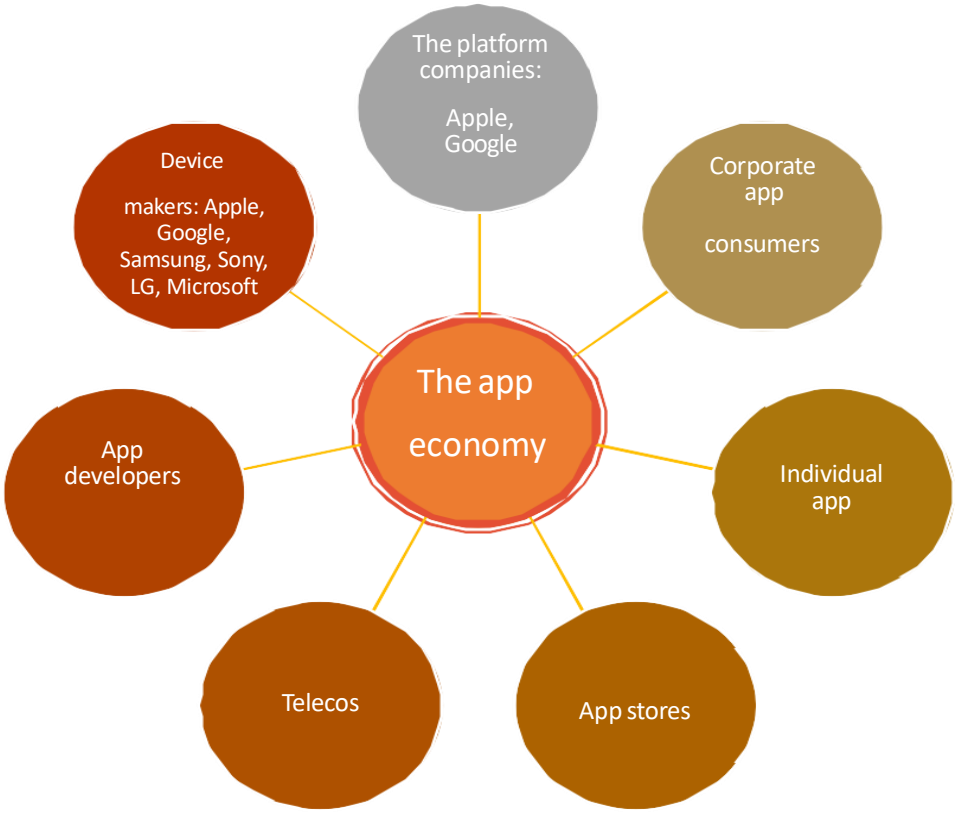
A. Issues Related to Regulatory Mechanism for OTT Communication Services

Q1: What should be the definition of over-the-top (OTT) services? Kindly provide a detailed response with justification.

Comments :

It is believed that the coinage of the term Over-The-Top commonly referred to as "OTT" stems from the fact that Over The Top communications bypasses traditional network distribution approaches and run over, or on top of, core Internet networks i.e. they operate over the top of telecom carriers rather than build their own communications infrastructure. A perceived negative connotation to the term Over-The-Top amongst other things has led to some proposing that the term

be changed to Online Service Providers (OSP) however this is not a generally accepted position. The impact of OTT services and the 'App Economy' more generally, has led to an expansion and a complexification of the information and communications ecosystem. Where previously the main players in the marketplace were simply carriers, handset manufacturers and consumers, now the market includes the giant platform companies, Apple and Google, a greater diversity of handset manufacturers, app developers and app stores and so on.



Although there is no generally agreed definition of Over-The-Top services however; many have made attempts at defining the term.

1. The Economic Co-operation and Development (OECD) refers to OTT as video, voice and other services provided over the internet rather than solely over the provider's own managed network. *(OECD Communications Outlook 2013/ Organisation for Economic Co-operation and Development 2013)*

2. Bertin, Crespi, L'Hostis (n.d) define an OTT provider as a service provider that offers telecom services, but that neither operates a telecom network nor leases networking capabilities from a telecom operator, relying only on the worldwide Internet network. *(A few myths about Telco and OTT models | Bertin, Crespi, L'Hostis (n.d.))*
3. The European Union (EU) broadly regards Over-The-Top (OTT) as an online service that can be regarded as potentially substituting for traditional telecommunications and audiovisual services such as voice telephony, SMS and television. It further distinguishes between OTTs, Online Services and Managed services noting that OTTs represent a subset of online services, which also differ from managed services. It holds that Managed services are those where the provider offering the service has substantial control over the fixed or mobile access network used for its distribution while Online services and the associated applications rely on the public Internet for at least parts of

their distribution. *(Over-The-Top Players (OTTs) / European Parliament- Directorate-General for Internal Policies 2015)*

4. In a paper presented at the Regional Economic and Financial Forum of Telecommunications and ICTs for Arab Region *(ITU Regional Economic & Financial Forum of Telecommunications/ICTs for Arab Region, Manam, Bahrain, 29 November 2015)* , the ITU refers to OTT services as applications and services, which are accessible over the Internet and ride on Operators' networks offering Internet access services e.g. social networks, search engines, amateur video aggregation sites, etc. While there is no single, generally agreed definition for Over-The-Top (OTT) services.

5. Canada's telecom regulator, stated that it "Considers that Internet access to programming independent of a facility or network dedicated to its delivery (via, for example, cable or satellite) is the defining feature of what has been termed 'over-the-top' services *". (Ref. "Results of the fact-finding exercise on the over-the-top programming services")*

6. The United States Federal Communications Commission (FCC) categorizes the OTT services into two groups: multichannel video programming distributors (MVPDs); and online video distributors (OVDs).

7. The FCC defined an OVD as:

> Any entity that provides video programming by means of the Internet or other Internet Protocol (IP)-based transmission path where the transmission path is provided by a person other than the OVD. An OVD does not include an MVPD inside its MVPD footprint or an MVPD to the extent it is offering online video programming as a component of an MVPD subscription to customers whose homes are inside its MVPD footprint. (Ref. FCC (6 May 2016*). Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming [Seventeenth Report; MB Docket No. 15-158; DA 16-510]*, *"FCC Officially Launches OVD Definition NPRM"*)

8. At the Caribbean Association of National Telecommunications Organizations (CANTO) meeting held

in 2014, where OTT was described as ‘a general term used for services that a customer may use which rides on top of a network to which the customer is connected.’ (CANTO 2014)

OTT services are grouped into three broad groups namely:

i. Voice over IP (VoIP) – for voice calling and video chatting services;

ii. Instant Messaging services- chat application; and

iii. Video and Audio Streaming services Although these OTT services are offered as either free or freemium services, consumers still require an active data connection and or subscription to enjoy these services. OTT players are not just enabling users to access their services at much lower cost and encouraging more users to opt for IP-based free or low cost services, they are increasingly introducing more innovative services in the communications market and as a result creating an increasing loyal user base. With the

increased use of mobile smartphones for payment to gaming, these OTT players are evolving beyond traditional messaging and voice, which are still the mainstream revenue streams for most operators.

(A) What are the Over-The-Top (OTT) services?

The term over-the-top (OTT) refers to applications and services which are accessible over the internet and ride on operators' networks offering internet access services e.g. social networks, search engines, amateur video aggregation sites etc. The best known examples of OTT are Skype, Viber, WhatsApp, Chat On, Snapchat, Instagram, Kik, Google Talk, Hike, Line, WeChat, Tango, ecommerce sites (Amazon, Flipkart etc), Ola, Facebook messenger, Black Berry Messenger, iMessage, online video games and movies (Netflix, Pandora). Today, users can directly access these applications online from any place, at any time, using a variety of internet connected consumer devices, also which includes,

(a) Applications and services which are accessible over the internet and ride on operators networks offering internet access services;

(b) Three types of OTT-

(i) Communications,

(ii) Video content,

(iii) Application eco system;

(c) Two broad categories of services-

(i) Communications and

(ii) Non Communications; and

(d) Three broad public policy issues-

(i) Regulatory imbalances,

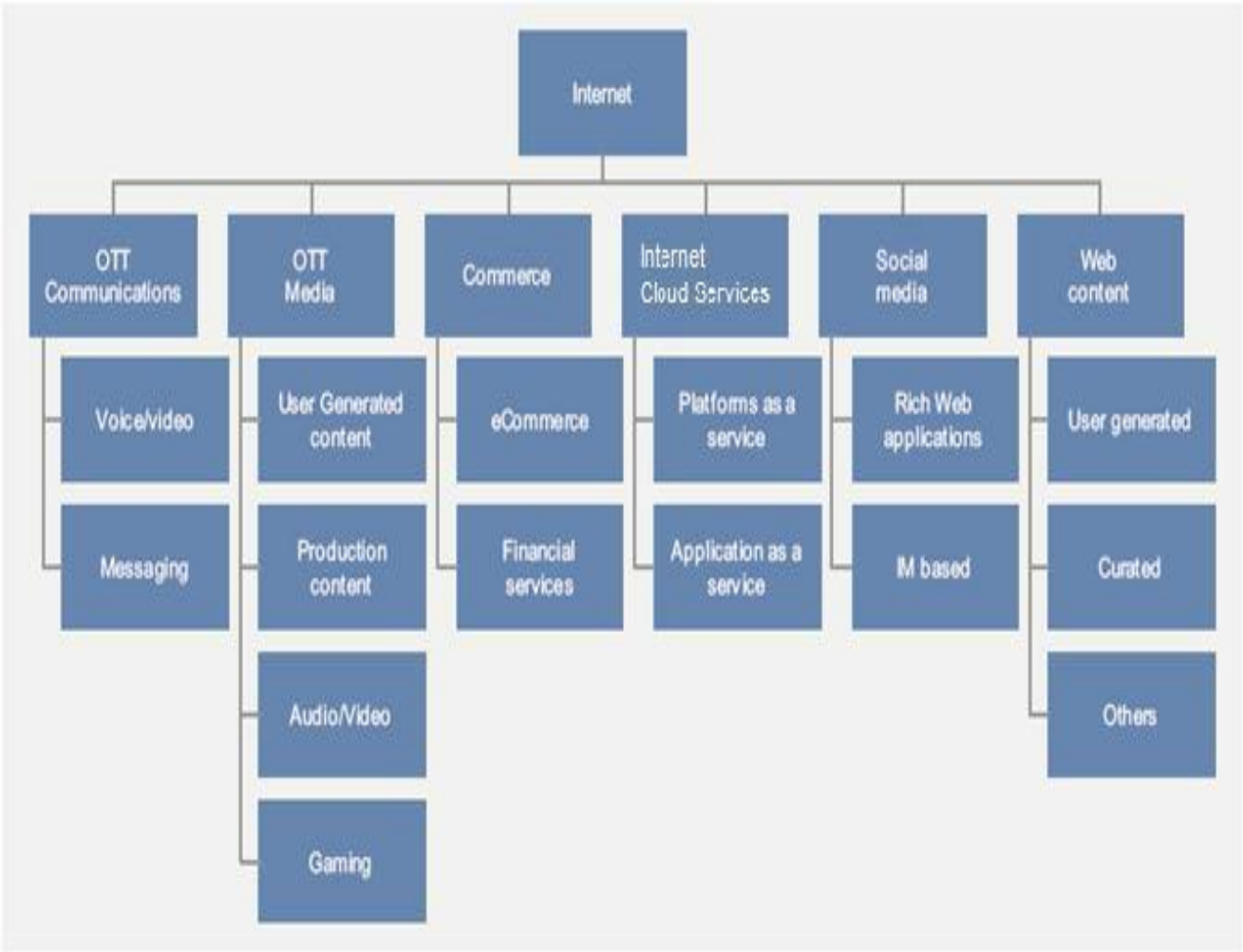
(ii) impact on economy and

(iii) security issues.

The services available on the internet can be broadly categorized as in Figure below. Apart from web content and

social media, OTT communications and OTT media are now increasingly playing a major role in the internet domain.

Internet Classification



An OTT provider can be defined as a service provider offering ICT (Information Communication Technology) services, but neither operates a network nor leases network capacity

from a network operator. Instead, OTT providers rely on the global internet and access network speeds (ranging from 256 Kilobits for messaging to speeds in the range of Megabits (0.5 to 3) for video streaming) to reach the user, hence going "over-the-top" of a telecom service provider's (TSP's) network. Services provided under the OTT umbrella typically relate to media and communications and are, generally, free or lower in cost as compared to traditional methods of delivery.

Section 2 (w) of Information Technology Act, 2005 —intermediary, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

Q2: **What could be the reasonable classification of OTT services based on an intelligible differentia? Please provide a list of the categories of OTT services based on such classification. Kindly provide a detailed response with justification.**

Comments : Mentioned above.

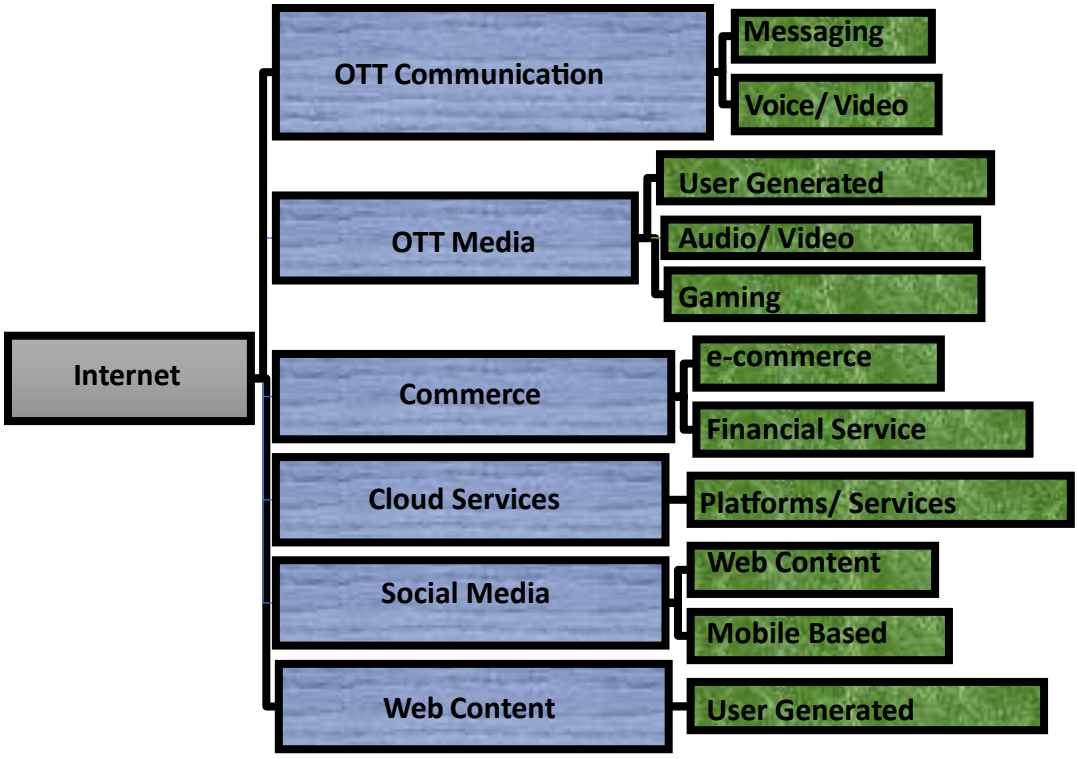
Q3: **What should be the definition of OTT communication services? Please provide a list of features which may comprehensively characterize OTT communication services. Kindly provide a detailed response with justification.**

Comments : Mentioned above.

Q4: **What could be the reasonable classification of OTT communication services based on an intelligible differentia? Please provide a list of the categories of OTT**

communication services based on such classification. Kindly provide a detailed response with justification.

Comments :



Q5. Please provide your views on the following aspects of OTT communication services vis-à-vis licensed telecommunication services in India:

Comments :

Areas of Regulation	Telecom Service Providers	OTT Players
Spectrum allotment and use	Need to bear costs and adhere to rules	No such costs
Licensing	Yes, different licenses and their associated costs including licensing fee	No such licenses or costs
Spectrum related charges	Need to bear the costs	No such costs
Space related charges	Need to bear the costs	No such costs
Bank Guarantees to the government	Yes	No
Proper record keeping including methodology	Required	Required through other acts
Interconnection	Yes, required as part of regulatory regime. Requirement to interconnect entails costs.	No such interconnection required as they are 'Over the Top' networks
Quality of Service Parameters	Required as part of regulatory regime	No such requirement
Obligations under various Telegraph Acts	Need to adhere to rules	No such requirement
Infrastructure sharing	Need to bear the costs	No Infrastructure sharing
Security conditions	Need to adhere to rules	No such requirement
Emergency and Public utility services	Need to adhere to rules	No such requirement
Monitoring services i.e. Lawful interception and monitoring	Required as a license condition	No such requirement

Regulatory aspects :

TRAI needs to focus on an area which is very relevant and necessary to protect and improve the areas as mentioned below which are connected to OTT's regulatory frame work :

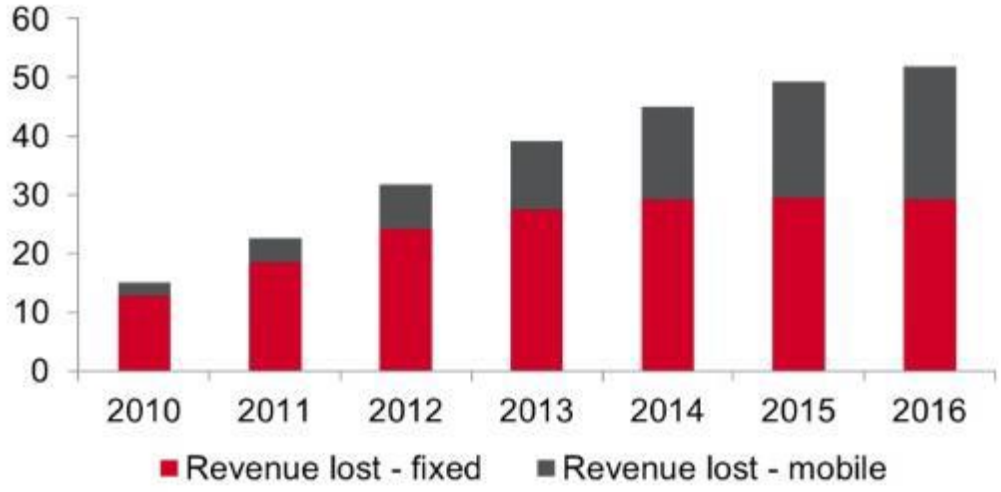
(a) Authorization and Licensing;

Telecom Service Providers (TSPs) are regulated by a number of laws, including the Indian Telegraph Act, 1885 (Telegraph Act), TRAI Act, 1997, the terms of the license agreement entered into between the TSP and the Government and the rules and regulations framed by the Government and TRAI from time to time. This section outlines some of the licensing obligations that are applicable to TSPs.

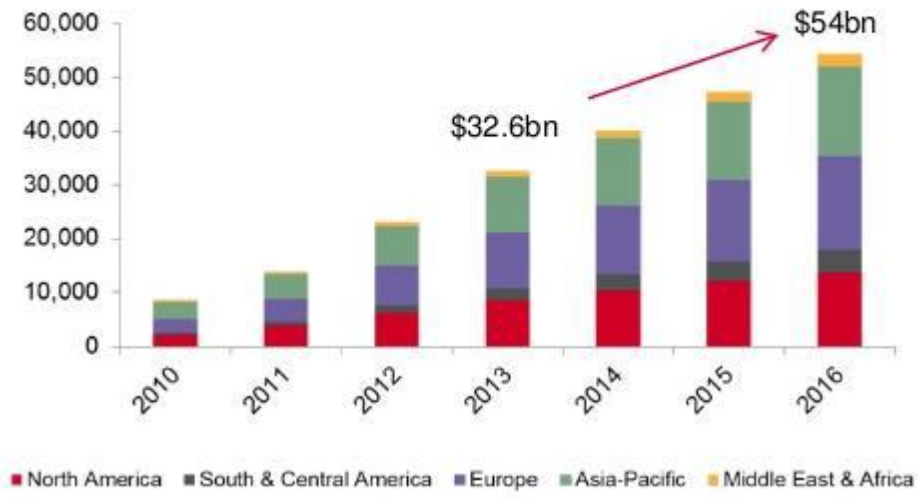
(b) Economic aspects :

Network Operators' Revenues Lost to OTT Players

Telco revenues lost to OTT VoIP: 2010–16 (US$bn)



Telco SMS revenues lost to social messaging: 2010–16 ($m)



- $52bn revenues are estimated to be “lost” to OTT VoIP globally in 2016

- Over $40bn SMS revenues lost to OTT social messaging in 2014

(c) Security aspects :

Comments :

The biggest security threat is from the select off-shore OTT communication service players which are highly capitalized, global monopolies and to day control multiple million customers across continents.

Issues related to security, safety and privacy of the consumer

- Cultural sensitivity and diversity as most of the OTT players operate from outside the country
- Loss of content privacy & compromised cyber security leading to cyber crimes
- Free apps share the personal information with various third party developers
- In constant 'always on' connections, what information is being collected by mobile apps. (Bigdata)

- Cyber predators, bullies, stalkers are alone line waiting to find their next victim.(Childabuse..)

(d) Privacy aspects :

TSPs are required to "ensure the protection of privacy of communication" and to ensure that unauthorized interception of message does not take place. The license agreement also restricts licensees from employing bulk encryption equipment in its network and mandates the ensuring of network security.

A number of OTT communication solutions do not support encryption. This implies that attackers can easily eavesdrop into an OTT service (such as VoIP conversation and IM services). In addition to the obvious problem of confidential information being accessed, the use of unencrypted VoIP and IM communication channels also facilitates identity theft or fraud. The other security threat concerns traffic analysis, which involves determining who is talking to whom. Such information

can be beneficial to cyber criminals preparing an attack, e.g. for committing corporate espionage.

(e) Safety aspects : Mentioned above

(f) Quality of service aspects :

In contrast, OTT service providers do not have to provide any QoS guarantees, instead QoS issues are blamed on network providers. Others however argue that OTT players also make efforts to improve user experience such as questionnaires at the end of VoIP calls which ask about the quality of user experience as well as their investments in data compression and quality of service. The Quality of Service (QoS) in OTT space largely depends upon the QoS of underlying telecom services. The former are offered as is with their consumption dependent upon consumer choice. The latter are controlled by regulation and also driven by consumer expectations;

(g) Consumer grievance redressal aspects :

Comments : Mentioned.

and

(h) any other aspects (please specify) :

Kindly provide a detailed response with justification.

Other Aspects :

(c) Country of Jurisdiction;

OTT services store, process and transfer data belonging to citizens or companies of one country in another country or countries. They usually collect data pertaining to call detail records and demographic details of users. This transfer of data across national borders creates issues. First, it creates ambiguity regarding the territorial application of data protections norms i.e. countries are unsure if the privacy of their citizens data is adequately protected when it is hosted in other countries. Secondly, this technology has made it difficult for law enforcement authorities to investigate or gather evidence in criminal and taxation matters, as evidence data may be hosted in a different jurisdiction from where the offence was

committed. OTTs situated in other jurisdictions may refuse to comply with request for cooperation or information sharing.

(d) Competition Law and Economics :

OTT Services are products of the permission less innovation that has made the Internet what it is today. These services are mainly free to consumer, but monetized through advertisement or other use of customer data, such as for development of technologies that are priced in future products. The telecom services are licensed and paid for directly by the consumer.

(e) Pricing Regulations:

Price regulation is imposed, especially on dominant operators that have the potential to abuse their market power and engage in anti-competitive practices. However, this form of regulation does not apply to OTT service providers who may possess similar market power which is equally subject to abuse.

(f) Taxing Regulations:

The lack of regulations allows OTT players to adopt innovative, flexible and agile business model, which are far more optimized. While many telecom operators/network owners are liable to pay taxes in every country they are operating in, such an obligation is not applicable to OTT service providers as they are, mainly required to pay taxes to the country where there main headquarters is located.

(g) Interconnection Regulations:

Many operators have raised concerns about the market share and power of major OTT service providers to be gatekeepers to attract content, instead of the operators themselves. Operators have claimed that by generating demand for bandwidth, OTT service providers generate expenses in (next generation) infrastructure investment, but have not made a fair contribution to these expenses through the 'interconnection' arrangements they make with telecom operators.

(h) Data Protection and Privacy:

The ability for operators to offer data protection and security as well as the means to enable interception of data (such as browsing histories, online purchases, e-mail or messaging communications) for law enforcement purposes are regulatory requirements imposed in most jurisdictions. While TRAI strictly monitor data protection and privacy requirements for users by operators, OTTs regulation is practiced on a rather limited and generally voluntary basis. OTT service providers face minimal regulatory constraints. The limits put on their business usually exist only to the extent of addressing the security and privacy concerns associated with user data. A number of OTT communication solutions do not support encryption. This implies that attackers can easily eavesdrop into an OTT service (such as VoIP conversation and IM services). In addition to the obvious problem of confidential information

being accessed, the use of unencrypted VoIP and IM communication channels also facilitates identity theft or fraud.

Q6. Whether there is a need to bring OTT communication services under any licensing/regulatory framework to promote a competitive landscape for the benefit of consumers and service innovation? Kindly provide a detailed response with justification.

Comments : Yes.

We are advocating a licensing and light touch regulation framework for OTT communication services like, WhatsApp, Signal, Telegram and other similar Apps. This realm of OTT communication Apps, not the entire ecosystem.

It will be important to provide clarity on the regulatory framework for OTTs, to meet the objective of sovereignty, compliance and growth.

Looking at the present scenario, the need for an unbiased regulatory body is a must. The Internet Content Streaming cannot be controlled by a self-regulatory body. The body shall distinguish responsible content for regulation. The OTT platforms, TRAI and the Government should work together on this and end this issue once and for all. At this point of time OTT platform is at a nascent stage across the globe. India needs to make sure that they cope up with the needs of the people while making a legislation.

The basic purpose behind the law should be clear; whether it is made to protect the audience or to bridge the regulatory gap. The Intermediary Rules, 2011 should also be kept in mind as violation of the Rules shall lead to cancellation of their license. Total censorship on the platform will transform it into nothing more than a television show or mainstream cinema. Also, it would lead to increasing cases of piracy.

The public today is looking for content that brings out the truth of the society, deals with socio-political issues, provides us regional varieties and utmost importantly doesn't hurt the sentiments of a single class of people. Hence, these regulatory gaps and grey areas are alarming.

Why is Regulation of OTT Communication Services Important?

- **Leveling the Playing Field Between TSPs and OTT Platforms:** It is important to create a **fair competition between telecom service providers (TSPs) and OTT platforms.**
    - TSP in India are regulated by several laws, including the **Indian Telegraph Act, 1885, the Wireless Telegraphy Act, 1933 and the Telecom Regulatory Authority of India Act, 1997.**

- TSPs have to follow certain rules and pay fees to the government for **providing voice and SMS services.**
    - They also need to **meet quality standards, ensure security, and protect consumers**.
- However, **OTT platforms offer similar services without facing these requirements,** which gives them an advantage.
    - Also, they do not contribute to the **Universal Service Obligation Fund (USOF).**
- This unfair competition **affects the revenue and profitability of TSPs and also impacts the government's revenue** from the telecom sector.

- **Lawful Interception and National Security**: Regulating OTT communication services is essential for national security and public order.
    - OTT platforms should be **subject to lawful interception and monitoring by security agencies** to prevent the **spread of misinformation, incitement of violence, or facilitation of criminal activities.**
    - Making OTT platforms responsible for any illegal content or activity on their platforms helps maintain a safe and secure online environment.

In case of VoIP OTT communication services, the reexists a regulatory arbitrage where in such services also by pass the existing licensing and regulatory regime creating a non-level playing field between TSP sand OTT providers both competing for the same service provision. Public policy response requires

that regulatory arbitrage does not dictate winners and losers in a competitive market for service provision.

The existence of a pricing arbitrage in VoIP OTT communication services requires a graduated and calibrated public policy response. In case of OTT VoIP international calling services, a liberal approach may be adopted. However, in case of domestic calls (local and national), communication services by TSPs and OTT communication services may be treated similarly from a regulatory angle for the present. The nature of regulatory similarity, the calibration of regulatory response and its phasing can be appropriately determined after public consultations and TRAI's recommendations to this effect.

India has, of late, seen multiple complaints against content on OTT platforms – such as Netflix, Amazon Prime and Disney+Hotstar.

While that happens, here's how other countries are dealing with it.

International Perspectives :

1. Countries like Singapore, UK have regulatory bodies to keep a check on the OTT platforms.

2. However, in UK, the OTT platforms face the same scrutiny as any public service broadcaster.

3. Australia has a principal legislation BSA, 1992 that governs the OTT sector.

4. While in Turkey, there is a licensing regime under which the OTT platforms are given a license for 10 years.

5. Countries like Indonesia, Turkey and Saudi Arabia have strict regulations. They want total control in the hands of Government. Many OTT platforms including Netflix has been blocked.

6. Indonesia :

   In August 2017, the Indonesian government via the

Ministry of Communication and Informatics (MCI) unveiled a liability framework for OTT providers. The sweeping regulations cover a whole slew of companies including SMS and voice calls and email services, chatting and instant messaging platforms, financial and commercial transaction service providers, search engines, social network and online media delivery networks, and companies that store and mine online data. The regulation, makes it mandatory for offshore businesses to establish a "permanent establishment" either through fixed local premises or by employing locals in their operations in Indonesia. **Transnational companies are also required to have an agreement with an Indonesian network provider, and use local IP numbers and national payment gateways for their services.**

The draft MCI regulations also require online platforms to create a **"censor mechanism" [sic] to filter and block "negative" content including terrorism, pornography and radical**

propaganda. While e-commerce and marketplace platforms enjoy immunity from content related obligations in Indonesia, the new regulation effectively dismantles this safe harbor framework.

7. Thailand :

Similar efforts to regulate online platforms are underway in Thailand. In April 2017, it suggested introducing bandwidth fees for online content providers, and has also proposed bringing OTT service providers under an operating license framework, taxing them for transactions by local merchants and **making them liable for illegal content.** In July 2017, the **Thai government issued an ultimatum to OTT services to register with the national telecom regulator** or face getting slapped with sanctions such as bans on advertising that would threaten revenue growth.

The Thai regulator is exploring a "complaints-based" framework of regulation and has set up a control list of the top

100 content creating companies that are required to establish local offices and be registered as entities in Thailand.

Efforts to create a "level playing field" could also be interpreted as measures to empower the regulator to more easily monitor and censor content that the government is finding difficult to regulate.

8. Singapore

The island nation has a body called the Infocomm Media Development Authority (IMDA) that requires service providers to obtain a license, while OTT services have a content code that ensures classification and ratings and a detailed list of prohibited content. If norms are flouted, the agency can withdraw content and impose penalties.

9. America

In 2019, there was a proposal for a new regulatory framework to monitor content on online platforms. The US

Federal Communications Commission (FCC) says the regulations were "unnecessary and heavy-handed" but was also seeking to introduce more practical regulations.

10. Australia

Australia's Communications and Media Authority (ACMA) for traditional media, while it has an 'eSafety Commissioner' for digital media. The content in the country is regulated by The Broadcasting Services Act, 1992 that has detailed guidelines, a complaint mechanism and a "refused classification" to be prohibited.

The phenomenon of regulating OTTs is not limited to Asia. In Latin America, several countries including Uruguay, Costa Rica, Colombia, Argentina and Brazil are considering legislative changes to enable the taxing of OTT players. In Argentina, the government has issued a set of principles for telecommunications regulation that create obligations for registration of Internet intermediaries.

The Zimbabwean President Robert Mugabe has created a Cyber Security, Threat Detection, and Mitigation Ministry to reign in threats emanating from social media. The government is also pressing ahead with a Computer and Cyber Crimes Bill, a comprehensive legislation that would allow the police to intercept data, seize electronic equipment and arrest people on loosely defined charges of “insurgency” and “terrorism.”

There may be various valid public interest reasons to regulate OTTs such as to ensure their compliance with privacy standards and net neutrality rules. But such regulations should be made on a targeted basis. Imposing a strict and unyielding regulatory framework based on telecommunications regulation and licensing goes further than this, and risks becoming a vehicle to protect legacy telcos and to enact content censorship.

International Legislations :

Singapore	France & Spain	UAE	USA	KSA
Specific Licenses for VoIP connecting to PSTN	OTT Providers are blocked when offering voice services that connect to PSTN	OTT only allowed they work with Licensed Telecom Companies	New FCC draft was released on March 12 2015 (will take few years to finalize)	OTT allowed only to work with Licensed Telecom Companies.

Good Practice :

- Traffic management is critical for the proper functioning of the Internet, but it can also be misused by an ISP to discriminates and create unfair access to the Internet and limit competition.
- Review of regulatory guidelines needed to curb some of the more harmful traffic management practices, such as total blocking and extended throttling, is critical- regulatory

action for curbing these practices should be evidence-based and in line with the harm suffered.

- Consistently monitoring of traffic management schedules and provisioning is critical
- Instituting guidelines for user-friendly switching to other providers who are not throttling is important.
- Publication of ISPs that engage in blocking and throttling is bearing fruit in certain markets, i.e. Canada.
- Increasing ISP competition and contestation on access markets is important – where the end users have limited options for an ISP (in a market where there two or less providers, competition is constrained).
- Strengthening transparency guidelines to empower and educate consumers is a great idea.

Conclusion :

With the demand-surge for data predicted to continue to grow, NN and related issues will be even more critical into the

future. Thus, the TRAI and policy-makers will need to review, taking into account the specific local market realities, the consequences (on competition, QoS/QoE, interconnection, investment in network capacity, small OTTs/app developers, consumer protection, etc.) of maintaining the status quo, of introducing light touch regulations or tweaks of the current NN rules, or even, of actively enforcing NN bright line regulation.

Q7. In case it is decided to bring OTT communication services under a licensing/ regulatory framework, what licensing/ regulatory framework(s) would be appropriate for the various classes of OTT communication services as envisaged in the question number 4 above? Specifically, what should be the provisions in the licensing/ regulatory framework(s) for OTT Communication services in respect of the following aspects:

Comments :

Command-and-control regulation of OTTs is definitely not advised, a light-touch regulation that imposes responsibility and liability on OTT service providers on their service offerings and privacy norms is definitely warranted.

A useful starting point for developing a framework for regulatory responses is to consider who are the winners and losers from disruption processes among the set of stakeholders in the communications market. Understanding where the costs and benefits of disruption fall is a guide to regulators about where regulatory relief for regulatory pressure can be applied (see Table below).

Below table shows how benefits and costs are redistributed in the app economy. Consumers, for example, have benefited from lower costs services and a wider range of innovative service offerings.

Table : Benefits and costs created and redistributed in the App economy

Group	Benefits	Costs	Outcomes
Consumers	– Better, lower price services – Wider range of innovative, content and services offerings	– More advertising – Loss of personal information (security and privacy) – Complaints	– Hugely positive for consumers
Non-comms businesses	– Better, lower price services – Increased competitiveness – New distribution and marketing channels increasing customer engagement	– Possibly reduced demand for outputs if telecommunications/ICT services increases as a proportion of GDP – Possible industry disruption	– Positive for business - except sectors disrupted
OTT or Online service providers	– More users, more revenues – Monetising personal info – Opportunity to initial public offering,(IPO) capital raisings, etc.	– Increased provisioning costs – May need to invest to address bottlenecks	– Hugely positive for OTTs
Existing fixed and mobile network operators, ISP, and broadcasters	– Increased demand for and revenue from data services – Falling costs due to simplification and move to lower cost IP infrastructure	– Reduction of revenue for legacy voice and SMS services – Loss of market power – Need for additional spectrum, investment to handle demand, congestion, quality of service	– Currently negative but increased Data demand may make positive – Partnering may be positive
National Governments	– Increased telecommunications/ICT efficiency – Increased penetration – Ability to provide government services online –	– Impact on taxation revenue & fees – Decreased capacity for regulatory intervention – Reduced ability to provide national security and policing – consumer protection	– Negative except in developed/tax haven markets where OTTs based
Country/ National level/ Economy wide	– Increased telecommunications/ICT efficiency & consumer welfare – Platform for the establishment of new and innovative disruptive businesses	– Increased imports, loss of tax – Reduced ability to pursue national objectives – Fragmentation of national markets and undermining of national culture/sport markets	– Variable depending on the country and its policies – Active policy setting required

Source: ITU, Regulatory Challenges and Opportunities in the new ICT ecosystem, 2018

For consumers on the cost side, however, there are concerns about privacy and the management of personal information in the availability of processes to resolve complaints. On balance, consumer behaviour would suggest

that consumers believe the overall benefits of the shift to OTT services has been highly beneficial.

This framework indicates various areas for regulatory focus, for example, the need to address taxation issues in relation to OTT players and measures to address the capacity of operators to continue infrastructure investment in the face of declining revenues. The literature on regulatory responses to the app economy is now expanding quickly *(Regulatory challenges and opportunities in the new ICT ecosystem, 2018)* . From such sources it is possible to develop a taxonomy of regulatory concerns that includes the following:

- licensing
- universal service
- taxation
- quality of service
- net neutrality
- data protection and privacy

- interconnection
- infrastructure investment
- international roaming
- content regulation
- spectrum management.

(a) Lawful interception :

Up until now, there were no such separate laws for the content available in the net, but there are some articles and sections from different legislations that provides some kind of regulations and they are as follows :

1. The first one is Article 19 (1) of the Indian Constitution which provides the right to speech and expression to all. Thereby, any person who wishes to express their opinions, thoughts, and ideas through online can do so subject to restrictions under Article 19 (2). These restrictions are

imposed for the social security, public order and maintenance of international relations.

2. Secondly, Indian Penal Code speaks about the punishments in certain cases. Section 293 punishes any person who indulges in the activities of selling and distributing any work of literature which is obscene, Section 295A punishes any person who has the intention of outraging the religious sentiments with malice, Section 499 punishes a person for releasing defamatory content and Section 354 is applicable when any person insults the modesty of a woman.

3. Then there is the Indecent Representation of Women (Prevention) Act, 1986 which prohibits the indecent representation of women in advertisements, movies, books, etc.

4. For the offence of child pornography there is the POSCO (Protection of Children from Sexual offences) Act.

5. Under the Information Technology Act, 2000 section 67A, 67B and 67C imposes fine and imprisonment to any person who transits obscene materials, sexually explicit contents including depiction of children in sexual acts and the Government under Section 69A has the power to block the access of certain material to public.

Apart from the above stated there is the Cinematograph Act, 1952 which provides provision for certification of movies for exhibition and also there is a self- regulatory code known as the 'Code of Best Practices for Online Curated Content Providers' released by IAMAI- Internet and Mobile Association of India.

Information Technology Act, 2000 (IT Act) :

(i) The IT Act and the rules framed under it place certain regulatory obligations on body corporates or intermediaries which includes TSPs and OTT services that can be regarded as

same/similar to the services provides by TSPs. They are as follows :

The Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. Also empowers the Central Government to monitor and collect traffic data or information through any computer resource for cyber security. (**Ref. Section 69B of Information Technology Act, 2000.**)

(ii) **Takedown obligations:**

Information Technology Act empowers the Central Government to issue directions to any intermediary for blocking for public access of any information in any computer resource. The provision also prescribes a punishment of imprisonment up to seven years for any intermediary who fails to comply with the direction issued under it. (**Ref. Section 69 A of Information Technology Act, 2000**)

(b) Authorization and Licensing;

Telecom Service Providers (TSPs) are regulated by a number of laws, including the Indian Telegraph Act, 1885 (Telegraph Act), TRAI Act, 1997, the terms of the license agreement entered into between the TSP and the Government and the rules and regulations framed by the Government and TRAI from time to time. This section outlines some of the licensing obligations that are applicable to TSPs;

(b) Privacy and security :

DATA PROTECTION AND PRIVACY :

In May 2016 the EU published the final text of the General Data Protection Regulation (GDPR) which came into force on 25 May 2018. The GDPR, one of the more robust and wide ranging privacy protection and data processing regulations, defines personal data as a piece of information (e.g. name, email address, IP address, social media profile, cookie address, location data) that is able to identify a person2. In addition, the official explainer of the directive emphasizes that “personal data that has been de-identified, encrypted or pseudo-anonymize but can be used to re-identify a person remains personal data and falls within the scope of the law”. (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en) In other words, wherever the identifiable personal information is stored is subject to the directive.

In order to protect personal data, the directive demands entities employ a number of techniques such as anonymization (masking personal identifiable information), pseudonymization

(using artificial identifiers to conceal personal data), and encryption to protect personal information. More importantly, the obligation is not only for the private data identifiers to be hidden or masked but also for personal data to be shared only on a strict 'need to know' basis.

Amidst unease about the harvesting and processing of personal data (e.g. the Cambridge Analytica scandal), the UK Information Commissioner's Office launched an inquiry in 2016 into the processing of such information. The enquiry was also in response to the growing global concern that electoral legislation has not kept up with the influence of digital and technological advancements on political campaigns. In another Commonwealth country, Kenya, their 2017 elections are another very interesting case study of the role of technology in electioneering. This is a perennial theme that emerges, i.e. the challenge that various key public services face in keeping up with digitization – whether in financial services (mobile money,

blockchain, etc.) or taxation (digital vs physical presence, intangible assets, etc.).

Unlike in the US, where third party data can be processed without active consent, in the EU area such a practice was prohibited even before the GDPR was in force. For instance, in February 2018, a Berlin court ruled that Facebook's default privacy settings and personal data processing violate German consumer regulations. It ruled that Facebook regularly neglected to properly inform users not only about the collection of the data, but also to provide users with adequate opportunity to offer consent for use of such data. (https://www.theguardian.com/technology/2018/feb/12/facebook-personal-data-privacy-settings-ruled-illegalgerman-court)

a) Data Protection and Privacy Trends :

The Internet, through a number of OTT services and apps, has enabled millions of people around the world to access the Internet to shop, be entertained, and to learn, amongst other activities. However, this online access also presents new

dangers. A relatively minor data breach can expose users to financial scams, cyber-bullying, grooming, profiling or being blitzed with spam and inappropriate content.

These dangers have inspired calls for the proper management of personal data protection and privacy, especially in light of the growth of OTTs. A number of specific policy issues about personal data protection and privacy have gained prominence in the last few years thrust in the headlines by the data analytics scandals referred to above but also the spectacular cyber data breaches and data protection failures. More recently, the WannaCry attack which, according to Wikipedia, affected 200000 persons and some 300 000 computers in 150 countries is a classic example. The hackers were paid a ransom, through Bitcoins, by the victims to regain access to personal data held hostage by the hackers. Also, Uber failed to report a major security breach on the personal data of 57 million customers and 600 000 drivers. The company is now

under investigation and faces civil damage claims. In 2017, Equifax, a leading consumer-credit reporting agency, experienced a data breach in which the personal information of 143 million mainly US consumers (but also Canadian and British customers as well) was accessed by hackers for several months. The personal information included the affected persons' names, birth dates, addresses, drivers' licenses and social security numbers.

These types of large-scale cyber-attacks are increasing in intensity and reach. The disquiet concerning the safety of personal data from, for instance, identity theft, goes beyond the proliferation of OTT services and applications. Most certainly, the concerns are even more pronounced in several OTTs (e.g. digital financial services such as Paypal and related online payment apps) that are not directly in competition with electronic communication services. It is clear that digital identity (and concomitant digital footprint) and personal

information are increasingly a considered prized commodity. It has been reported by cyber-security companies that a growing number of fraudsters are pursuing leads on digital files of personal information ahead of financial or even physical assets.

All these unsettling developments are taking place against the background of terrorist attacks in Europe. Consequently, several European governments, have demanded a revision of the end-to-end encryption (calling for "responsible encryption" that allow law enforcement authorities to tap into conversations, and be provided with "backdoors" or special keys to unlock personal encrypted messages, especially on WhatsApp and other related messaging services to address terrorism and related issues. (http://www.wired.co.uk/article/uk-encryption-whatsapp-amber-rudd)

What are the policy tools and regulatory process to address these challenges? Since, data breaches do not respect national borders, what international security infrastructure is in place to

protect users and safeguard privacy online? We should think over it.

b) Policy and Regulatory issues :

The EU's GDPR is significant because of its extensive reach and extra-territorial application. The EU is emphatic that the GDPR is applicable to all international companies (both EU and non-EU business) – even without physical commercial presence in the region – handling the personal data of EU citizens. These requirements will persuade developers and programmers around the world to re-think their data protection rules and revise existing protection systems to embed the Privacy by Design principles in the operations, as outlined in the directive. This extra-territorial applicability effectively elevates the GDPR to a global data protection regulation. Many countries around the world are reviewing and amending current national legislation to address issues highlighted by the EU directive.

The definition of personal data has, on the whole, been fairly extensive but the GDPR expands it to include new types of personal data (e.g. cookie ID) as outlined above. The implications of such a comprehensive reach is that a whole host of organizations and entities (whether in financial services, health sector, online retail, entertainment industry, etc.) will be obliged to comply with the requirements of the GDPR. Many organizations, whether in the OTT ecosystem or in the broader ICT industry, would have to invest in robust IT systems, as well as, develop appropriate policies and processes to enable early detection of data breaches and adequately protect personal data. It has been alleged that certain the social media app, Facebook on Android still logs users calls and texts. (https://www.tomsguide.com/us/facebook-logs-calls-texts,news-26847.html)

The GDPR introduces a stricter client consent system – the directive demands that entities that have access to personal information seek consent from end-users about the specific personal information they collate and archive. Also,

organizations and institutions are required to explicitly underscore the option to opt-out, i.e. automatic opt-in is now restricted. More critically, silence from the user does not constitute consent. Similarly, entities with personal information are required to detail the reasons for collecting personal data, and more importantly, openly disclose the intention to share the information with third parties. Essentially, end-users, including of leading OTTs such as Facebook, Twitter and YouTube, are empowered to control the rights to their personal data.

More interesting, the EU directive endorses the right to data privacy – in Article 17, the GDPR reenforces the concept of the right to be forgotten or the right to erasure. In other words, organization are required to provide a legitimate cause for gathering and archiving personal data. Further, end users are empowered to request access to archived data, portability of the data, or even complete deletion. Users are empowered to

object to the use of their personal data for advertising or research purposes. The data processing company is required to immediately cease to use the personal data if, and whenever an objection is lodged, or show compelling and legitimate public interest in processing the said data.

Also, the GDPR demands that Data Protection Officer be appointed, by public authorities processing personal data, as well as, as organizations that regularly handle and process large sets of personal information (OTT companies are considered included in this category), to ensure active compliance with the directive. Compliance is demanded in the collection, storing, sharing and use of the personal data.

Furthermore, the GDPR has harmonized the notification guidelines for data breaches in the EU area – a data breaches is to be notified within 3 days. It is required that the data-breach notification detail the nature of the breach, the number of users affected, and the type of information accessed. Similarly, most

US states already have data breach notification laws in place, while Australia has just enacted (February 2018) a new data-breach notification regulation which demands of organizations to promptly report the breaches that put lives at risk – the targets of the disclosure is the affected persons and the Office of the Australian Information Commissioner (OAIC). (immunization and school health records are held by the Family Educational Rights and Privacy Act)

The French and Spanish data protection authority, have already published detailed guidelines for industry to comply.

Finally, the GDPR demands data protection by default and design (PbD). In order to protect personal data companies are required to develop relevant policies and put in place appropriate technological capacity. The PdD framework were first advanced as a best practice in Canada in the 1990s by the Ontario Privacy Commission to address the quick-fix approach to data breaches. The GDPR demands PbD as a default on all digital applications and services.

The most significant part of the directive is the penalty and liability for the data breach – the penalties could be racked up to 4% of the global turnover for a breach of data or violation of the consent system.

In order to protect the personal data and privacy of users of OTTs and other online apps, the following are critical:

- Data security issues transverse national borders and are not limited by physical jurisdictions – thus, international cooperation and harmonization of legislation on privacy and data protection frameworks are crucial.
- Intra-country cooperation between various intersecting e-government databases, such as health, education, immigration units
- Participation all the key stakeholders in developing personal data protections policy and principles

- Developing and adopting industry wide standards to inculcate a culture of cybersecurity awareness is not an option
- Outlining regulatory regime and institutional frameworks for protecting personal data
- Fostering a culture of cybersecurity through consumer education and empowerment
- Digital literacy, intended to equip users with tools, knowledge and skill to navigate online life including managing online privacy settings, from an early age is becoming increasingly imperative
- Updating current criminal prosecutions regime to align to the digital reality

In Nutshell :

Digital identity and personal information is increasingly a considered prized commodity by OTT service providers and by legacy networks, as well. Consequently, efforts underway at

national and regional levels to discipline the processing of personal data are important. However, the EU's GDPR, because of its extended jurisdiction and comprehensive approach to personal data protection, is rightly the focus point for global discussion, especially for countries that do not currently have comprehensive data protection regulations. A number of principles rights and obligations in the regulation, i.e. the rules on obtaining valid consent for processing personal data (in which companies are not only required to obtain user consent using simple and clear language, but to also clearly state how the personal data will be used) will affect how OTTs, as well as, legacy networks handle individuals data.

Policy and Regulation :

In the past, universal service and access policy objectives were mostly focused on providing voice telephony services. However, with recent technological innovations (e.g. increased availability of smart phones and internet services which enabled

the rise of OTT services) universal service and access now includes broadband. More significant, the EU's universal service and access directive mandates that universal service obligations be reviewed every three years.

It bears recalling that very recently regulators were administering a scheme very similar to what some of the telcos are demanding. What the telcos are calling for is similar to access deficits charges – the concept that access rates, whether interconnection or termination are not high enough to cover the network costs of providing the service – in connection to OTT services. Interestingly, the ITU has noted that almost all of these access deficit charges are being revised because of the "wrong incentive" they facilitate. In fact, these charges are being "phased out in most countries [Malaysia, Russia and India] where they were previously adopted. It is also said that in the face of fierce competition such 'subsidies' may do more damage than good.

(c) Emergency Services :

Since OTT services need not interconnect with PSTN, they are not obliged under regulation to provide emergency services. Though there are third party services exist that enable OTT services to provide emergency services, it is not mandatory.

This is regarding the emergency and safety services that are provided by the TSPs on a priority basis as implemented in 911 or Enhanced 911 in the U.S. for a long time. Though such stringent quality regulation is not present in India for emergency services, when you call 112 it is the responsibility of the originating carrier of the call to connect to the nearby ambulance, fire and police departments. This feature is absent on OTTs. In the U.S., the emergency services provisioning is extended beyond wireline and wireless carriers to Interconnected Voice over Internet Protocol (VoIP) service providers that permits users generally to receive calls that originate on the Public Switched Telephone Network (PSTN) and

to terminate calls to the PSTN. As TSPs have now been allowed to provide unrestricted Internet Telephony, it is time that we define whether emergency services should be provided only by carriers but also by the Interconnected VoIP providers (i.e. TSPs who provide VoIP services) and OTT service providers! One such mechanism is to mandatorily require OTT service providers to connect to PLMN/PSTN switch, thereby interconnecting with the Telco network for carrying emergency calls.

(d) Unsolicited Commercial Communication :

"Tackling UCC on WhatsApp should be relatively easier. It's a closed system unlike SMS and users can easily block a number since it is not interoperable and is app to app.

The move also comes at a time when the government has questioned some of WhatsApp's practices including the lack of tractability of messages to check and stop circulation of fake news. WhatsApp has been slapped with two notices by the IT ministry on the issue related to circulation of fake news, and

has thereafter taken several measures, including adding 'forward' label to help users identify such messages.

The company however has not accepted the demand by the government to trace the origin of such messages as it believes that creating a software for such a purpose will go against its user privacy policy and end-to-end encryption.

OTTs do self-regulate in stopping UCC on their platforms, the "fake news forwards" and unwanted advertisements have come to haunt consumers.

It's time OTTs are brought under UCC regulation due to their large-scale adoption. Otherwise, we will be left with a regulated UCC for limited TSP messaging and a self-regulation for the burgeoning OTT messaging.

(e) Customer verification :

In the past decade or so, technology has undergone a vast change, which has also impacted the entertainment industry as

it is a huge medium that guarantees maximum popularity in India and abroad.

However, the OTT revolution changed everything, as everything began to be available on OTT (over-the-top) platforms.

OTT platforms have seen a massive rise in viewership in the past few years, although its users have to deal with several security issues as well due to OTT services falling prey for revenue frauds and identity thefts.

This is why OTT verification is important as it confirms the users' identity via use of digital verification technologies, through which content providers can verify the correct user.

Identity fraud has been a common practice with many users creating fake identities or impersonating real people to subscribe to OTT platforms for the sole purpose of enticing and committing fraud by luring innocent victims into their trap.

Therefore, every OTT platform needs to have a User Identity Verification through which millions of identities can be managed without compromising user experience.

The way broadcasters and content providers distribute content has drastically changed within the last couple of years. With a significant increase in audiences flocking to OTT platforms in the last year, the media industry has undoubtedly changed everyone's leisure time.

However, the sudden increase in users on OTT platforms has also increased a number of challenges broadcasters and content distributors face when it comes to how viewers view their content. One of the biggest challenges these platforms face is centered around security and conversion. How can broadcasters and OTT players ensure that their omnichannel experiences are secure enough to ensure that that only those

who are paying or subscribing to the platform have access to the content.

Unfortunately for platforms that only require a simple password login, password sharing and identity theft have long been issues that have cut into the pockets of providers. Today, content distributers need to put their best foot forward to securely authenticate and authorize users to avoid and eliminate any possibility of any user sneaking into the network that may lead to financial losses or brand reputation tarnishing.

No one likes to remember long credentials, especially if they can utilize the true potential of frictionless login across all applications and connected devices. While SSO is on the verge of becoming an industry standard for authentication, OTT platforms need to quickly gear up for enhancing the user experience through SSO and Federated SSO.

With the growing count of data breaches and stolen identities throughout the world, OTT platforms should consider implementing a strong authentication solution.

Authentication has become critical in creating a seamless omnichannel experience across different devices or maintaining billions of identities.

The Department of Telecommunications (DoT), should plan to create an obligation on telcos to share know-your-customer details of their users with over-the-top (OTT) communication platforms like WhatsApp **and Signal.**

“Such a provision will help OTTs display the verified name of a caller which will help in reducing impersonation and frauds,” said a source.

It is likely to create an obligation on both telcos and OTTs to have the verified name as part of caller line identification.

The government has included provisions in the draft version of the telecom bill that came out in September, to protect users from 'specified messages'. The bill has defined this as 'any message offering, advertising or promoting goods, services, interest in property, business opportunity, employment opportunity or investment opportunity.'

Such measures can also include measures relating to the prior consent of users for receiving certain types of messages, and the preparation and maintenance of 'Do Not Disturb' registers so that users do not receive such messages without prior consent.

We have seen that, the government has been receptive to OTTs' concerns over being clubbed with telecom service providers for all kinds of regulations in the bill.

(f) QUALITY OF SERVICE (QOS)/QUALITY OF EXPERIENCE (QOE) :

The ITU has been defining QoS and QoE standards for decades. In the ITU's Definitions of Terms Related to Quality of Service [ITU-T Rec. E.800 (09/2008)] Quality of Service (QoS) is defined as the "totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service." (ITU (2008), Definitions of Terms Related to Quality of Service E.800 Series, p. 3) The ITU has, in various QoS and QoE standards, articulated the criteria of seven parameters to measure performance of service and applications against agreed expectation.

The parameters in QoS are:

- Accuracy (e.g. low packet corruption; correct accounting and billing)
- Availability (e.g. network coverage for mobile telephone)
- Flexibility (e.g. to switch between service providers; multiple bill payment systems)
- Reliability (e.g. low packet loss)

- Simplicity (e.g. user-friendly services such as clear billing statement)
- Security (e.g. personal data security)
- Speed (e.g. fast connection; prompt resolution of subscriber complains)

In addition to measuring QoS, statistics on Quality of Experience (QoE) performance as experienced by the end-user (as opposed to QoS which measures network delivery), are just as critical. The importance of monitoring QoE will be increasingly significant as end-users do more data-heavy online activity (e.g. video streaming for entertainment or distance-learning applications) which is sensitive to transmission speed and jitter.

In some senses, the customer perceptions of quality and the digital experience are integral to the growth of the Internet, and the impact of OTTs is significant. OTT services and applications (such as Skype, WhatsApp and Viber) have been

driving positive consumer experience and customer satisfaction metrics – in terms of affordability, content, innovation, app functionality and features, amongst other performance benefits.

The ITU's newly revised definition of QoE is that it is "the degree of delight or annoyance of the user of an application or service" (ITU (2017) Quality of Service Regulation Manual, Geneva, Switzerland, p. 12), as delivered through the network. In ITU parlance, QoE measures the mean opinion score (MOS), based on statistics collected through customer surveys, in which one (1) is bad customer experience and five (5) is excellent quality experience. MOS used to measure voice quality but has now been expanded to include video-television delivered via Internet protocols. QoE, evidently subjective, is impacted on by a number of variables including "the type and characteristics of the application or service, context of use, the user expectations with respect to the application or service and their fulfillment",

amongst other issues. Thus, the end-users impression of quality is not only about the interface with the device or the equipment delivering the service, but also the personal experience as the service is consumed. In a nutshell, QoE is dependent on QoS as well as users actual experience against expectation.

In summary, QoS and QoE metrics/indicators monitor the quality performance of services and applications provided, as well as, the end-user experience of what is supplied. The quality metrics are both objective and subjective.

Policy and Regulation :

TRAI should constantly monitor scheduling priorities and compliance with specific QoS performance levels –

a) to enhance quality access to internet services

b) to assess that network degradation is limited

c) to safeguard the interests of end users by ensuring that network optimization measures are not employed to restrict competition.

Further, by setting and enforcing QoS standards, the TRAI will hopefully persuade the network operators to further invest in robust network capacity and innovative network optimization tools including the Internet Engineering Task Force (IETF) defined traffic management protocols (such as the Integrated Services and Differentiated Services models) to enhance end-to-end QoS in IP environments.

TRAI that monitor and enforce QoS and QoE provisioning should :

- Conducting public awareness campaigns about quality standards does not only empower end users to make informed decisions about service offerings, but also increases transparency, accountability and provides a valuable feedback loop.

- Interconnection, Net Neutrality as well as Network Performance are inextricably linked, and have impact on QoS and QoE indicators.
- The IP connections (main platforms transporting OTTs), which by design only deliver best-effort service, straddle different networks. Thus, guaranteeing end-to-end QoS and QoE in the varied IP-based environment is challenging given that several transport technologies will have different QoS and QoE provisions. Furthermore, QoS and QoE obligations in licensing agreements are addressed differently by different regulators, dealing with different network capacities and infrastructures.
- International standards, designed to boost end-to-end QoS in IP environments, are a great starting point to harmonize regional quality standards.

In Nutshell :

QoS and QoE indicators have evolved with the transition from circuit-switched networks to IP-based platforms to now include indicators on performance of multimedia services. However, IP-based systems present a challenge with regards to measuring end-to-end QoS. As pointed out above, quality standards are influenced by a number of parameters and protocols along the Internet value chain. Thus, has regulation on QoS and QoE kept up with these changes in relation to interconnection between operators, net neutrality guidelines defining Best Effort delivery, or even QoE indicators for end-users? Are the current minimum QoS and QoE standards adequate for data-heavy applications, such as multimedia apps, which demand guaranteed bandwidth in a best effort IP network? QoS solutions for both OTTs and managed services, in IP environments, are increasingly critical, and answers to these questions will impact on the growth of the data ecosystem.

(g) Consumer grievance redressal;

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules), was the first attempt to provide a dedicated framework for the previously unregulated OTT sector. It envisaged the creation of a three-tier grievance redressal mechanism which included a government body at its third level.

(h) Eligibility conditions;

The fundamental difference between the OTT service providers and the TSPs is in the ownership of the network, and the concomitant responsibilities for maintaining and upgrading that network to meet quality of service (QoS) standards. Whereas TSPs face all of these responsibilities as part of their license obligations, OTT service providers do not have a license and face no such obligations. The aim of OTT regulation, should be to restore regulatory balance.

(i) Financial conditions (such as application processing fee, entry fee, license fee, bank guarantees etc.); and

Comments : No Comments.

(j) Any other aspects (please specify).

ADDITIONAL COMPLEXITY IN THE TRANSITION TO AN IP WORLD:

In addition to the many regulatory issues identified above, transition to an IP world involves additional complexities that arise from the more complex structure that communications markets are currently evolving into and fact that, beyond communications, the app economy is influence almost every aspect of economic and social life.

1. THE COMPLEXITY OF TWO-SIDED MARKETS AND CROSS-INDUSTRY PLAYERS :

One of these complexities is the increasing importance of two-sided markets. Commercial terrestrial free to air television is the most common example of such a market structure. In

effect, television networks produce audiences and sell these audiences' attention to advertisers.

Two sided markets are the basis of the business models for companies such as Google and Facebook. The lack of direct observable transactions and prices in such markets means that it is more difficult to assess the efficiency of these markets and define profit margins as inputs to regulatory decision making.

Another factor affecting the complexity that regulators must contend with is the fact that OTT offerings are not restricted to communications markets. Over the past five years the most significant impact on broadcast television markets has been the rise of Internet-based streaming video services. High-resolution video content is a significant network capacity and consumers are increasingly viewing video content on mobile devices. In addition to streaming services, social media platforms are increasingly populated with video content which is typically viewed on mobile devices. This expanded presence

of content being transmitted by the telecommunications system rather than via broadcasting, raises issues of content control and classification that broadcasting has contended with throughout its history.

2. GLOBE-SPANNING NATURAL MONOPOLIES :

The issue of market structure is particularly problematic in the context of the app economy. While regulators are familiar with the problem of natural monopoly at the local or national levels, OTT players are transnational monopolists or oligopolists and these are intrinsically difficult to address with legislation and regulation based on national jurisdictions.

Scale is a key driver for app economy players and given the inherently unlimited scalability of the software and hardware systems that underpinned their services, the monopoly power of these players can only be expected to grow. It is likely that many of the areas of activity or submarkets in the digital economy will be natural monopolies or at least highly

concentrated oligopolies. This is because so many factors are driving global level scale. In addition to the unlimited scalability of computing systems, businesses like Facebook and Uber have strong network externalities characteristics – more users mean better services with more features and therefore more reasons to join. In addition, given the size to which the leading companies in each submarket have grown, new challengers, even if they are highly innovative, tend to be snapped up before they become a competitive threat.

3. SOCIAL, CULTURAL AND POLITICAL INFLUENCES :

Discussion on the social cultural and political aspects of social media and Internet publishing and new sources is now widespread and daily news in its own right. Issues such as fake news, political manipulation to the level of interference with electoral processes, and exposure to potentially harmful content. These issues impact different countries in different ways. For example, non-Western cultures may view exposure to

various types of content carried over social media, streaming or simply available on the World Wide Web, as being incompatible with their cultural norms. There are also similar challenges in relation to religious sensitivities and content.

4. OTT SERVICES IN DEVELOPING COMMONWEALTH COUNTRIES

Commonwealth countries span an enormous range of economic development as indicated by GDP per capita and their levels of ICT maturity also vary enormously as measured by the ITU's ICT Development Index.

As mentioned above, telecommunication services can play a critical role in accelerating economic development in less developed countries. Information is the lifeblood of markets and bringing even modest communications services to previously underserviced populations can accelerate the process of transitioning from subsistence to market-based activity.

As communications technologies evolve and become more sophisticated and efficient, and the infrastructure becomes cheaper to deploy, telecommunications can have larger impacts sooner on lower income populations. For this to be achieved it is critical to activate and maintain to the communications infrastructure investment and to ensure that sufficient investment funding is available for new technology upgrades. For this reason, the impact of OTT services on operator revenues and margins is of particular concern in less-developed countries.

An additional factor affecting regulatory approaches to OTT services is the fact that in many less developed countries governments still own operators, often monopoly operators, and operator earnings form a significant component of overall government revenue.

Detailed Analysis of Key Regulatory Issues and Recommended Options :

THE IP REGULATORY AGENDA :

As indicated above, the regulatory agenda for responding to OTT services and, more broadly, the evolution to an IP everywhere world, is broad indeed. Given this broad agenda it is extremely important to prioritize.

We have grouped the following regulatory topics under the headings critical, important and desirable:

Critical for Regulatory Attention :

- content regulation
- licensing
- data protection, privacy, user control of data
- universal service provision

Important for Regulatory Attention :

- spectrum allocation
- interconnection
- quality of service
- net neutrality

Desirable for Regulatory Attention :

- international mobile roaming.

In addition to these more traditional telecommunications regulatory concerns, there is the additional issue of taxation of OTT providers. This challenge is cross jurisdictional in two senses: it requires international cooperation and it requires collaborative regulation as espoused by the ITU which brings together regulators from various regulatory and administrative arms of national governments.

CRITICAL FOR REGULATORY ATTENTION

1. CONTENT REGULATION :

In the past ten years the proliferation of affordable smartphones, and increasingly ubiquitous wireless broadband networks has resulted in enormous disruption of the traditional content delivery models of newspapers (first), and now broadcasters are being disrupted by digital content providers. Ensuring a level playing field between old and new content

distribution models has also been difficult with prevailing local content rules, cultural requirements as well as taxation and licensing requirements being inconsistent, dated and often adhoc.

Regulatory frameworks, therefore, must evolve as markets evolve, it is not possible to regulate the future into the past. Flexibility in adopting regulatory approach is arguably the key, but there is little doubt that new arrangements, approaches and tools will be necessary. *(Refer to ITU Paper " The Challenge of Managing Digital Content" for the 'ITU-TRAI Regulatory Roundtable', 21-22 August 2017, New Delhi, India. Available at https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/August-RR-ITP-2017/ITU%20Report%20Regulatng%20Digital%20Content%202017%20Final.pdf)*

Historically, the focus has been on the traditional media platform – television, radio, film and print. However, the emergence of digital streaming services has led to revaluation of key concepts typically used in the regulation of content. This is now the subject of numerous reviews in Commonwealth countries.

Digital content available to consumers can generally be divided into two categories,

(i) Commercial content and

(ii) User-generated content.

These categories are not mutually exclusive and products where there is subscription content over social media platforms are evidentiary of both categories.

2. REGULATORY ISSUES ASSOCIATED WITH DIGITAL CONTENT:

Social media companies have created OTT services used globally and intended to positively benefit individuals worldwide. However, the introduction of social media has also seen a proliferation of troubling content. Social media platforms have been used to spread terrorism propaganda and used as an outlet for violent content. The ability to distribute such content sparks concerns amongst policy makers. There is limited

liability for social media platforms that aid users in distributing illegal content.

Social media platforms have also caused copyright infringement issues, especially with live broadcasts of sporting events. Live streaming is a potential threat to the future viability of live sporting events, and to the sustainability of live television broadcasts generally.

Social media platforms such as Facebook, Twitter and Google have arguably morphed into some of the world's biggest publishers and broadcasters. With this new role of social media as a news source, a specific concern has been the effect of false stories – or 'fake news' – circulating on the Internet. News shared through Social media platforms typically have dramatically different structures from and operate in different legal frameworks than traditional media organizations, meaning that content can be relayed among users with no

significant third-party filtering, fact-checking, editorial judgment or legal liability.

In some Commonwealth countries such as Sri Lanka, in March 2018, arguably due to the lack of response from OTT players sought to block access to Facebook, as well as two other platforms that Facebook owns, WhatsApp and Instagram, in an attempt to reduce violence directed at its Muslim minority. As use of the social media platforms has accelerated in recent years, so have cases of extremist fringe groups using Facebook's reach to magnify their messages. In 2017, India blocked a number of social networking services— including Facebook, Twitter, WhatsApp and YouTube — for one month in the disputed territory of Jammu and Kashmir in a bid to curb street protests there.

3. GLOBAL MEASURES FOR REGULATING DIGITAL CONTENT: GENERAL

There are a number of critical focus areas that have been addressed by organizations and national regulators globally. The ITU launched the Child Online Protection ('COP') Initiative in 2008 within the framework of the Global Cybersecurity Agenda ('GCA'), aimed at bringing together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere. (www.itu.int/newsroom/press_releases/2008/33.html) Regulators globally have begun to streamline content regulation and complaint-handling procedures in response to the ineffectiveness of current complaint procedures. The European Council is considering a more demanding approach, requiring companies to block videos containing hate speech and incitements to terrorism. (www.theverge.com/2017/5/24/15684168/eu-hate-speech-law-facebook-twitter-youtube- video) This will be beyond the current imposition and implementation of the General Data Protection Regulation (GDPR). The UK and France have joined forces to tackle online radicalization with plans, such has creating new legal liability,

that could lead to much stronger action taken against social media companies who fail to remove unacceptable content. (www.gov.uk/government/n ews/uk-and-france-announce-joint-campaign-to-tackle-online-radicalisation)

As pressure from governments heightens globally, including in the United States social media companies and ISPs have also taken steps to further improve self-regulation of their platforms. Facebook, Microsoft, Twitter, and YouTube have launched a partnership in June 2017 aimed at combating terrorists online. (www.theverge.com/platform/amp/2017/6/26/15875102/facebook-microsoft-twitter-youtube-global-internet-forumcounter-terrorism) Further developments following the allegations of interference in the US election have resulted in further calls for regulation in that market. (www.cnet.com/news/congress-isnt-ready-to-regulate-zuckerberg-facebook-twitter-google/)

In light of the perceived ineffectiveness of complaint procedures by the main social media platforms (eg including Facebook, Twitter, Snap, etc) combined with the importance of

efficiency in taking dangerous and illegal content down, it is recommended Commonwealth countries formulate legislative amendments which would streamline content regulation and complaint-handling procedures to make them as efficient and effective as possible. Those domestic law processes or mechanisms (e.g. a court with a cyber jurisdiction or a special Commissioner with certain special delegated powers in relation to take-down orders for content that, for example, involves terrorism or child pornography) should is consistent with international norms and is readily understood by global OTT players.

There should be an agreed single point of contact for interfacing on such requests which should typically be the Commonwealth country's telecommunications regulator unless a specialist country regulator is created such as Australia's e-Safety Commissioner. Importantly, the optimal approach to

regulation in this new digital environment is not more regulation, but rather, better regulation.

4. OTHER MEASURES FOR REGULATING DIGITAL CONTENT:

In a significant departure from the traditional licensing of broadcasters (and of telecommunications network facilities and services), several countries have sought to license Internet content providers. One approach adopted in Singapore, a Commonwealth country has been specific amendments made to licensing rules to require country specific internet news content within the individual licensing regime.

Irrespective of where the content is hosted and/or whether the publisher has a presence in Singapore, an Internet site is required to be individually licensed under the Singapore Broadcasting Act 1994 (as amended) if it meets the criteria in the Notification. Such an approach to licensing if promulgated would provide the any Commonwealth regulator with regulatory

tools it may not have previously had because of the hosting location of material.

(i) Policy and Regulation

In short, regulators employ the regulatory tool of licensing to achieve a number of objectives including to :

(a) Establish regulatory certainty and ensure predictability

(b) Encourage investment in network roll-out and telecommunications service provision

(c) Ensure efficient deployment of scare resources (e.g. spectrum allocation)

(d) Mandate quality of service obligations and consumer protection guarantees

(ii) Trends in Licensing :

The telecommunications sector has, in the last few years, been undergoing radical changes, which pose a challenge to regulators throughout the world. These developments, such as the convergence of previously separate applications such as

voice, video and data streaming (from a single network as opposed to multiple networks) into a single data flow, demand an update of the regulatory and licensing regime. Having grappled with a few regulatory questions and policy issues, as a result of these innovations, regulators throughout the world reflected on the possible trajectories of these fast-evolving technologies. What has been clear is that predicting the path of technological advances and the long terms trends of the sector, with any degree of certainty, is challenging for regulators.

Consequently, regulators around the world have been steadily reducing the regulatory conditions attached to licensing, in recognition not only of convergence trends, but that licensing processes impose costs (e.g. bureaucratic delays, administration overheads, etc.) for both the regulator and the licensee. Also, authorities are appreciating that easing licensing requirements has been shown to boost market access and competition. The ITU argues the technology implications of the

transition to Next Generation Networks means that "*fair competition between different network infrastructures demands a technology neutral licensing regime*." Moreover, that, a "*unified licensing will stimulate optimal use of technology options by operators*."[22]

Hence, licensing fees, whether calculated as a portion of the annual turnover or per subscriber, have been coming down in the last few years. In India, after steadily increasing with the boost in subscriber numbers, the license fees were later simplified and revised downwards by the TRAI following an evaluation by the Bureau of Industry Cost and Prices. *(https://cis-india.org/telecom/resources/licensing-framework-for-telecom)* Also, following a number of consultations with industry, the United Kingdom's Office of Communications, or Ofcom, revised down, annual license fees for mobile spectrum. *(https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/annual-licence-fees-mobile-spectrum)*

Many regulators have been transitioning away from service

and technology specific licensing regimes to introduce certain flexibilities, and/or even eliminating the licensing requirements altogether – and so, opening up the market to new players and new technologies. For instance, Japan eased the regulatory requirements extensively – currently, there is no tariff regulation, and furthermore, a simple registration and notification is sufficient to provide internet services and certain value added services in the country. *(http://www.ictregulationtoolkit.org/practice_note?practice_note_id=726)* In place of these licensing conditions, the Japanese regulator strengthened the consumer protection regulations, and importantly, transferred the administrative and financial burden of addressing consumer complaints to the service providers.

Some countries, such as the US and China, even allocate certain bands of spectrum without a license, to boost wireless technologies for broadband access. Japan has assigned the 57 GHz to 66 GHz spectrum for use without a specific license.

Other regulators, such as in the European Union (EU) are recommending limited regulatory conditions for provision of services, or what is referred to as general authorizations. Instead the regulators conduct periodic evaluations and impact assessments of the policy choice on the market developments. Yet other countries such as Nigeria, India and Egypt have opted for unified, generic and technology-neutral licensing regimes which permit the supply of communications services without specifying the type of infrastructure to deliver the service, or sometimes, even the type of service offering to be provided.

Following a public consultation and appointment of a consultant to undertake a market analysis of the new licensing regime, the Nigerian Communications Commission (NCC) published the relevant regulations observing that:

> *"… the Nigerian Communications Commission (NCC) issued a notice on the introduction of a unified licensing regime in Nigeria.*

It stated that:

- *The market shall be opened up by adopting a unified licensing regime which shall allow existing fixed wireless and mobile licensees to provide both services subject to geographical/regional limitations contained in their license*
- *For the post exclusivity period all wireless licenses shall not be segmented in terms of mobile and fixed service categories. Once a spectrum is allocated, licensees shall be free to offer voice, data or multimedia services as they deem fit.*
- *All active wireless licenses issued prior to the expiration of the exclusivity period shall be amended accordingly."* (https://www.ncc.gov.ng/docman-main/lic ensing-documents/434-licensing-framework-for-unified-access-service/file)

(iii) Good Practice :

The entry of OTTs to the market has raised a number of

regulatory questions and policy issues which need to be addressed. For instance:

- What are the implications if regulators completely eliminate market entry restrictions (especially in markets where the incumbents still have significant market power), expressed through a licensing regime, (as Japan has partially done)?
- Also, how do regulators address the issues raised by the legacy network providers while ensuring that the technological innovations and the competitive elements introduced by the entry of OTT service providers continue to accrue to end-users?
- How does regulation maintain an optimal balance between the incumbents and the new entrants?
- Further, which regulatory tools are best suited to protect consumer interests (or even extend universal service obligations without revenue from the license fees) outside of the licensing regime?

- Is licensing the best regulatory instrument to impose regulatory obligations?

Re-regulation through licensing (as envisaged by some ICT industry players) would seem to go against the liberalization trends introduced by the convergence program. Further, re-instating licensing would appear to be inconsistent with the underlying values that inform the 'light touch' regulatory arrangements embraced in the last few years. Will re-licensing impose legacy network regulations (mostly designed to countervail the power of an incumbent with a significant market power), to new technological advances and market place realities?

There is no silver-bullet answer to these critical questions, but a few tried-and-tested principles seems to inform the approach of a number of regulators as they address rapid market changes in the telecommunications sector. These principles are detailed below:

(e) Committing to service-neutral and technology-neutral forms of regulatory regimes – experience suggests that such an approach encourages competition and take-up of new technologies

(f) Encouraging investment in networks to engender a healthy telecoms market primed to provide affordable, trusted and quality services to end-users

(g) Ensuring that consumer protection underpins key regulatory decisions

(h) Committing to consultation, transparency and procedural fairness in all the regulatory amendments envisaged

(i) Remaining adaptable and dynamic – being agile and responsive to the technological changes taking shape is critical

In Nutshell :

The Body of European Regulators for Electronic Communication (BEREC) concedes that even though the ideal is

a level regulatory playing field, "there can also be reasons for different regulatory treatment of services". BEREC goes on to state that:

> *"The range of services to which any specific obligation should apply, must be considered in light of the goals of the obligation and the proportionality of that obligation being applied to any specific service or service type. The proportionality of that obligation and its scope follows from whether the social benefits of the obligation are proportionate to the economic costs entailed for each regulated provider, and the static and dynamic competition effects of partial or universal application of the obligation. A preference for a level playing field can be part of the assessment of proportionality, but it is only one of the many elements."* (BEREC (2016), *Report on OTT Services* BoR (16) 35, p. 4)

The regulator should continue to walk the tight rope of

balancing the need to provide certainty for investors through a set of codified regulatory requirements on the one hand, and the flexibility demanded by a fast-evolving telecommunications sector on the other. Sector legislation in the countries should provide flexibility so that licensing of OTT players is possible. However it should be noted that such licensing make have the desired policy outcomes in larger markets it may not work for all markets. There are also strong arguments for the licensing burden and costs imposts on network operators to be eased in order to allow them to better compete with OTT players.

Inter Connection :

In some markets, the competitive environment has not matured enough to warrant a regime of minimal rules, but learning on the way forward regarding interconnection rules suggest the following :

- Provides regulatory guidelines (with strong competition bias) in advance on interconnection
- Ensure parity with regards to the level of quality of service provided to competitors, especially where access to infrastructure and networks is still unequal and potentially discriminatory
- Monitor network planning and provisioning schedules, ascertaining that planning is responsive to growth in demand, especially for OTT services and applications
- Define guidelines for proper management and storage of end-user information between the OTT providers and the networks providing interconnection services along the value chain
- Review interconnection pricing unresponsive to the technological advancements (which boost efficient use of network) ensuring that wholesale interconnection fees reflect cost

- Promote investment network infrastructure such as internet exchange points in developing countries
- Negotiate international interconnection principles to guide peering agreements in the interests of developing countries

Regulating interconnection is said to be a relatively complex and technical area of regulation – preparing guidelines for negotiating interconnection agreements can be time-consuming, and monitoring whether the agreements comply with the regulatory guidelines is difficult.

In relation to VoLTE it is clear that profound change to access regulation is required: VoLTE and IP based interconnection will result in fundamental rewriting of rules and pricing models for interconnection and access. More work is needed with TRAI and operators need to undertake extensive review of technical, financial, regulatory aspects, and

international roaming issues to explore implications, specifically:

- There is a need to adapt rules and costing/pricing models for an IP interconnection model. If set by a costing study there are likely to 30 percent, or lower than currently mobile termination rates. If such terminating rates are going to be significantly reduced then there may be commercial value in removing the cost of interconnection billing systems and moving to an IP peering arrangements after all voice as a percentage of total network traffic is falling substantially;
- Interconnect capacity (and any associated rules) between networks also need to change to move away from E1s with multiple network points of interconnection (POI) to a smaller number of IP connection points perhaps only 2 or 3 are needed in each domestic market. Possibly, any

regulatory rules prohibiting such changes may require amendments; and

- VoLTE international roaming which is an all-IP solution and may involve –Internetwork Packet Exchange (IPX) peering depending on the technical solution adopted – necessitates in changes to roaming arrangements, pricing or other regulatory requirements (eg legal intercept, access to emergency calling by roamers etc).

Q8. Whether there is a need for a collaborative framework between OTT communication service providers and the licensed telecommunication service providers? If yes, what should be the provisions of such a collaborative framework? Kindly provide a detailed response with justification.

Comments : No.

During the early days of satellite television in India, broadcasters had to partner with local cable operators and pay

them a hefty carriage fee in order to reach millions of TV households. The broadcaster-distributor partnership became more formal with the onset of direct-to-home services, while carriage fees became more structured, under-reporting disappeared and ARPU increased, making the partnership profitable for everyone. In recent years, the action has shifted to video streaming platforms or what are called over-the-top (OTT) content services. While the core game remains the same – since distribution remains critical for all content creators – the players have changed.

OTT services started gaining popularity in India in 2018 and have since been witnessing a growth in adoption. OTT operators continued to explore new ways to attract and monetize services. One of these strategies has been to partner with telecom operators to bundle content offerings and woo customers. This has not only resulted in an increase in the country's mobile data consumption, but has also caused a

significant shift in users' video-viewing habits, creating a demand for original India-focused shows and laid the foundation for a robust digital content ecosystem projected to be worth more than $5 billion in the next five years.

The telco-OTT partnership :

It all started when Reliance Industries Limited (RIL) acquired a 25 per cent stake in Balaji Telefilms and then partnered with ALTBalaji (a subscription-led OTT platform) under a content sharing deal in 2018. ALTBalaji was required to make its original shows available on Jio Cinema and Jio TV, enabling Jio's entire audience (160 million then, now 280 million) to enjoy their content. Following the Balaji deal, RIL turned its attention to Eros Now, another home-grown OTT service run by Eros International (a traditional movie producer and distributor). RIL acquired a 5 per cent stake in Eros to build and grow businesses around the content ecosystem. Following

the deal, Eros Now's multi-language entertainment library was made available on Jio TV and Jio Cinema.

Taking Jio's lead, Airtel partnered with Amazon to offer one year of Amazon Prime membership to all Airtel Infinity post-paid customers, providing over 300 live TV channels and 6,000 movies and shows. Airtel also extended these benefits to its V-Fiber broadband customers, giving wider access to these services. Airtel also bundled its Netflix service with three-month post-paid plans for a limited period. Moreover, it signed a partnership deal with Hotstar to make Hotstar's content available on Airtel TV -over 100,000 hours of content across live sports, movies and TV in nine languages – for free.

Vodafone, too, started offering a two-month subscription to Netflix and Amazon Prime for free to its RED post-paid customers. It offered a range of content through a single access point, Vodafone Play, to reduce not only entry barriers but

increase convenience for end-users. Moreover, Vi collaborated with Hungama to launch a pay-per-view model for premiering digital films from Hollywood at a one-time cost. The importance of telco-OTT partnerships was further solidified when state-owned Bharat Sanchar Nigam Limited announced a one-year free Amazon Prime subscription for its broadband and post-paid customers.

Win-win for operators and OTT players :

There was a time when value-added services constituted a major source of revenue and a competitive advantage for telecom companies. Now, telecom players have turned to OTT platforms to replace outdated value-added services. The association with telcos is a win-win for OTT platforms and telcos alike. It helps OTT players gain market share by increasing their advertising video-on-demand and subscription video-on-demand numbers, while telcos gain revenue per user by consuming more data.

Since most OTT players are losing money, partnering with telcos is helping them generate revenue and grow their subscriber base at the same time. Despite the fact that less than 1 per cent of 225 million OTT viewers pay for content, analysts feel that operators with their estimated 425 million data subscribers provide a huge potential to reach viewers not covered through these platforms.

Moreover, bundling OTT services has benefited operators through reduced churn and higher ARPU due to increased viewership of paid content, with Indian mobile subscribers now willing to pay a slightly higher price for these services. In addition, operators have valuable customer data that OTT platforms can use to tailor or match their content with their audience base. This is valuable data that can assist OTT platforms in marketing and refining their offerings.

Another reason is that mobile phones provide the easiest access to OTT content among all smart devices. Anyone can access content whenever they want, instead of being at home in front of a device. By connecting other smart devices to the same service, such as smartphones, smart TVs and gaming consoles, users can easily continue to stream content from one device to another. It makes sense for OTT platforms to partner with telecom operators to tap into their mass bases of smartphone users. With this access, OTT providers will be able to provide users with an access point to their content and a seamless experience of content consumption.

Moreover, partnering with telecom operators allows OTT platforms to overcome one of the biggest challenges in the industry – having to pay separately for each OTT platform, which is not appealing to most consumers. When partnering with a telco, billing and payment are handled by the telco through direct carrier billing. This allows OTT players to focus

on what they do best – finding and developing the best content for their audience.

According to Counterpoint Research, telecom operators pay OTT platforms like Zee5 for their content, and the payment terms are based on how much traffic they drive. OTT players usually have a defined budget and viewership target. In general, if the number of users accessing the platform exceeds the set target, the telecom operators will pay them extra for the additional users. Pixights Consulting states that telecom is one of the cheapest and most legitimate ways to get new OTT subscribers. As OTT platforms merge with telecom operators, the viewership of ad-supported content goes up, adding to OTT players' advertisement revenues. Alt-Balaji, which has used this partnership model, gets the majority of its subscribers through telecom operators.

The way forward

As per the 2020 EY-FICCI media and entertainment industry report, the Indian telecom industry will become the primary platform for content distribution and consumption in the years to come. The market is expected to grow to $4 billion-$5 billion by the year 2025.

OTT and video streaming platforms in India may be expanding, but they are far from being profitable. Without deeper partnerships with telecoms operators, OTT players in India face a challenging future since the majority of India's 600 million internet users consume free, ad-supported content.

For instance, Netflix launched a mobile-only Rs 199 monthly subscription in India in 2019 and appears to be testing an exclusive Rs 349 subscription for households that do not have TV sets – a significant percentage of India's population.

Going forward, OTT-telco partnerships in India should move from simple bundling to a strategy that enables deeper collaboration in order to grow sustainably. These strategies can involve joint product development and delivery of co-branded products as OTT players relying only on their telecom partners for distribution and new user segments are becoming increasingly unsustainable. Operators now package access to a variety of OTT platforms with their own telecom services, effectively commoditizing these services. In addition, OTT players can benefit from the influx of new audiences from Tier 2 and Tier 3 cities as well as older adults, which can allow them to reach a broader audience.

"We believe that there is much that both OTTs and TSPs have to gain from each other. There is a strong case for an even stronger relationship between them to emerge given the continued and exponential consumption of data in India at the lowest rates globally. In the short term there will be some pain

for the TSPs and there needs to be a mechanism to address this. One of the other issues that needs to be addressed is the democratization of hotspots across the country. We need to provide our rural population an even greater immersive experience via their smartphones – across not just entertainment but also health, education and a range of other services."

"Just as mobile transformed India, OTT is the next dimension of change. OTT services have added to the GDP of the country as well as to the productivity of people. This is in addition to the other benefits that they deliver to the TSPs at a time when their revenue from voice is zero. OTT is a very powerful and necessary lever for TSPs and ISPs as revenue generators. TSPs must be provided relief from excessive levies and taxes to ensure that they're healthy. TSPs create a value for whole of economy and hence their financial health is important for the whole of Indian economy to grow and prosper. Thus,

there is a need to create an ecosystem that is a win-win for them and all other stakeholders in their ecosystem. Also, OTTs do not fall under the Telegraph Act. In conclusion, we would say that both need to work together to advance Digital India's goals."

The root cause of the issue between OTTs and TSPs was not related to competition but due to legacy issues being faced by the telecom sector that were hampering investments in the sector. These issues relate to high levies and duties, onerous licensing conditions and spectrum pricing. The Indian Telegraph Act does not apply to OTTs – central to the Telegraph Act is the concept of owning, establishing, operating maintaining a telegraph which, as defined in the Telegraph Act, is what attracts licensing. OTT's do not own, establish, operate or maintain a telegraph – so the question of attracting licensing does not arise.

The discourse on policies towards OTTs and TSPs is far from settled. However, it may be considered that in the case of new generation internet-based services that have significant socio-economic impact, – it would be premature to pass hard rules. Careful and planned approaches to soft law can be attempted and later developed into more firm rules as the sector matures.

Q9. What could be the potential challenges arising out of the collaborative framework between OTT communication service providers and the licensed telecommunication service providers? How will it impact the aspects of net neutrality, consumer access and consumer choice etc.? What measures can be taken to address such challenges? Kindly provide a detailed response with justification.

Comments :

In May 2019, ITU-T vide its recommendation D.262 on 'Collaborative framework for OTTs' has recommended to

Member states for taking certain initiatives which inter-alia include developing enabling policies and/or regulatory frameworks to foster fair competition between network operators and providers of OTTs. Many member states and Sector Members have submitted contributions to propose ITU Studies on various aspects of OTTs. Regarding cooperation between OTT providers and telecom operators, various discussions are going on in the ITU forum.

OTT service providers should participate in infusing investment in the telecom networks by working out commercial arrangements with TSPs and allowing TSPs to offer OTT packs to consumers.

If telecom operators are to develop a successful strategic response to the rise of OTT competitors, they must first take stock of the considerable assets and capabilities they already possess, and determine how they can leverage them in order to compete against, or work with, the OTT players. These

strengths fall into two main categories. First, operators excel at providing ubiquitous connectivity over both fixed and wireless networks — a capability that has cost them huge sums of money to develop, and that no one else possesses — and ongoing upgrades to their next-generation networks will give them the ability to provide a variety of advanced services. These include upgraded traffic management and tiered quality of service, "big data" and customer analytics, advanced security and location-based services, and sophisticated cloud computing. Second, they maintain a dense, fully integrated, and scaled-up distribution footprint. This includes their strong retail network, with the ability to reach millions of users; supply chain and logistics services; an established billing and CRM relationship with their customers; and the ability to collect huge amounts of demographic, behavioral, and usage information about their customers. These assets allow operators to offer selected OTT companies access to their distribution footprint and to the

customer relationships they have already established. At the same time, however, operators are typically siloed organizations, structured to focus on subscriber and revenue growth within a specific product or channel. Their inherent focus on short-term profitability, coupled with the conflicting priorities across the various business silos, makes it difficult to achieve consensus on a consistent strategy. This is in distinct contrast to how OTT players operate. Because they don't have to worry about maintaining and investing further in basic technology infrastructure, OTT companies can concentrate on quickly building out and bringing to market highly innovative products and services through rapid prototyping, a "good enough" perspective, and frequent new releases.

Despite the OTT players' advantages in focus and innovation, the assets and capabilities that operators possess should enable them to take part — to some degree — at every level of the OTT opportunity. However, their success will

depend in large part on their ability to shore up their current business and then focus their strengths on the pools of value where they have a real chance of gaining ground.

The threat to telecom operators posed by OTT players is real, and operators need to consider how they plan to respond. In the long run, however, the two camps must understand that there's a growing pool of value to be shared and that they need each other. Operators control the networks that enable OTT businesses, and as their core business matures and markets reach saturation, they need new revenue streams to keep funding the network expansion that the OTT companies need to thrive. And in launching the digital businesses of tomorrow, OTT players will need fast, intelligent networks that can form the basis for a wide range of new services and provide their customers with the best possible experience. That's why operators looking beyond the desire to protect their core business are best advised to consider the business enabler play,

which depends for its success on creating value for OTT players to the benefit of all. Despite the challenges the operators face, they cannot afford to let the situation deteriorate into a win-or-lose proposition. To capture their share of the new value being created through digitization, operators need to adjust their world view, consider their position and preferred way to play in the OTT value chain, and develop the capabilities needed to win. And they need to move now.

Net Neutrality :

While there isn't a specific regulation currently in place, there have been recommendations for tackling illegal online content. A European Union paper on "Illegal and harmful content on the Internet" listed content that can be concerns to national security and some that can be a threat to impressionable minors as content which needs to be checked.

The phenomenon of regulating OTTs is not limited to Asia. In Latin America, several countries including Uruguay, Costa

Rica, Colombia, Argentina and Brazil are considering legislative changes to enable the taxing of OTT players. In Argentina, the government has issued a set of principles for telecommunications regulation that create obligations for registration of Internet intermediaries.

OTT Services and net Neutrality :

Table below summarizes the regulatory position taken in various countries in respect of Net Neutrality and OTT services.

Country	Position on OTT Services	Position on Net Neutrality
Eastern Caribbean Telecommunications Authority (ECTEL)	Has not published a position on OTT services.	Supports the principle of Net Neutrality. Views blocking and throttling as a practice that interferes with regional objectives. Reiterates that traffic management techniques by ISPs must not interfere with users' privacy rights and must not be used to achieve anticompetitive practices. ECTEL promotes information transparency to treat with the traffic management technique known as Deep Packet Inspection (DPI).
Trinidad	No formal position on OTT services. The regulator in its consultative document recommends no blocking of OTTs.	No formal position on Net Neutrality.

Country	Position on OTT Services	Position on Net Neutrality
Jamaica	No official position on OTT services. Authorities instructed Digicel and Flow to discontinue blocking of OTT mobile apps, Viber and Nimbuzz, after learning that the telecom operators had engaged in that traffic management practice that contravened the legal framework.	No formal position on Net Neutrality.
Barbados	Barbados has an established policy on VoIP services based on different classes of services. VoIP operators whose services that traverse the PSTN in any form must adhere to some kind ofregulatory obligations as explained above.	No formal position on Net Neutrality. Created policy for treatment of VoIP services before Net Neutrality became a global concern.
Canada	No formal position on OTT services. ITMP policy would apply to OTT services since OTT is viewed by the Canadian regulator as "Internet access to programming, independent of a facility or network dedicated to its delivery."	The policy is allowing for ITMP. Operators are required to state the ITMP being used; the need and purpose for the utilization of that ITMP, and the effect resulting from employing it when faced with questions relating to compliance. The Canadian Regulator, CRTC, has decided to take a complaints-based approach for instances of

Country	Position on OTT Services	Position on Net Neutrality
		infractions of this policy with the burden of proof being placed on the citizens and Internet users' association.
United Kingdom	No formal position on OTT services but has in the past advised telecom operator to desist from blocking Skype traffic to preserve the principle of Net Neutrality.	Seeks best-efforts' Internet access and the provision of managed services to co-exist. Would consider imposing a minimum quality of service on all communications providers if managed services were prioritised in a manner that leaves insufficient network capacity for 'best-efforts' access to the Open Internet. Relies on market forces to effectively address blocking and traffic management in a discriminating manner. Will keep the position under review. Requires technical information be available to consumers and transparency in traffic management.

Country	Position on OTT Services	Position on Net Neutrality
Brazil	No formal position on OTT services. Brazil boasts over 100 million WhatsApp subscribers making it a country with one ofthe largest subscriber base.	In April 2014 the for President of Brazil signed into law the Marco Civil da Internet Bill (Marco Civil) guaranteeing Internet privacy and ensuring the neutrality of the Internet. However, the bill allows for the following exception to Net Neutrality under conditions such as: i. cases when technical requirements necessitate exception for correct delivery of services and applications; and ii. for the prioritization of emergency services.
European Union	No formal position on OTT services. Analyzing whether or not OTT services are to be treated as an electronic communication service in accordance with the appropriate framework.	The EC implemented the following measures via the amended Universal Services Directive to bring about an environment that would eventuate in the buttressing of Net Neutrality that would mandate National Regulatory Authorities (NRA) to meet the following objectives:

Country	Position on OTT Services	Position on Net Neutrality
		i. "be able to set minimum quality levels for network transmission services (Article 22(3), Universal Service Directive); ii. allow consumers to be able to switch between ISPs quickly and without unnecessary penalties (Article 30, Universal Service Directive); and iii. ensure transparency in relation to ISPs' utilization of any traffic-shaping measures in their contracts with consumers (Article 21(3) (d), Universal Service Directive)." (GSR12 Discussion Paper)
The United States of America	Net Neutrality rules inform the position relating to OTT services.	**Previous Position on Net Neutrality:** In March of 2015, the FCC under Title II framework adopted three (3) rules called the Clear, Bright-Line Rules with the purpose of driving the concept of the Open

Country	Position on OTT Services	Position on Net Neutrality
		Internet, while also promoting innovation and investment in network infrastructure. These rules build on rules previously adopted. The rules include the following: i. Clear, Bright-Line Rules (i.e., No Blocking, No Throttling, No Paid Prioritization); ii. No Unreasonable Interference or Unreasonable Disadvantage to Consumers or Edge Providers; and; iii. Enhanced Transparency **New Position on Net Neutrality:** In December of 2017, The FCC, the US regulator of electronic communications, adopted the *Restoring Internet Freedom* Order. Some of the major changes are highlighted below: i. In the new Order,the FCC reclassified broadband Internet access service as an

Country	Position on OTT Services	Position on Net Neutrality
		information service, removing rules associated with the previous version such as the Clear Bright-Line and Internet conduct rules. ii. Also, The FCC modified the transparency rules by removing many reporting obligations, and restored the Federal Trade Commission (FTC) as the authority to prohibit unfair and deceptive practices, and protect interests of consumers.

Table 1: Summary of the current position by Country on Net Neutrality and OTT services[15]

B. Issues Related to Selective Banning of OTT Services

Q10. What are the technical challenges in selective banning of specific OTT services and websites in specific regions of the country for a specific period? Please elaborate your response and suggest technical solutions to mitigate the challenges.

Comments :

Difficulties in Selective Banning :

It is clear from the below discussion, **selective blocking though a theoretical possibility is practically not possible to execute on the ground.** Though the intent is novel, however, the side effects are too high for any of the options to be considered for execution. Middle way should be find out.

The idea is to prevent customer agony as a result of the blanket ban on Internet services to restore law and order. The intent of selective banning is to prevent some OTT applications (like WhatsApp, Face Book, Telegram Etc) from

operating while leaving others untouched. The purpose of this note is to analyze whether an optimal blocking strategy exists which can balance all dimensions of business — cost, customer experience, and privacy.

1. Normal Blocking

Before we discuss the selective blocking of OTT services, let's understand how normal blocking of internet services works. This the operators do through a technical process called PCRF (Policy and Charging Rules Functions). This is nothing but a set of service rules that the operator applies to the specific set of BTSs (Base Stations) that it intends to block. **Through this rule, the targeted BTSs can be set for zero or very low data rates,** so that all kinds of data services emanating or targeted towards them get throttled — making them useless. Note that PCRF does not discriminate between various data applications and it is also agnostic to IP addresses. It is simple to execute and is very cost-effective.

Selective Blocking (OTT level) :

Selective blocking of OTT applications can get executed either at the OTT player level or at the telecom operator level. Now for the OTT player to block services in a specific geography it will need the location information of all the users. **The location information can be at the GPS level or at the Cell ID level.** Accessing both these pieces of information will pose significant challenges.

In order to execute GPS level — All the devices have to be GPS-capable. In fact, most are not. Even if they are, the OTT player has to seek permission from the user to access it. **Now if sharing is made mandatory (through a govt mandate), it will create havoc** — Everyone's location will get tracked all the time and the user will have no choice but to move without the device to ensure privacy. **Cell ID tracking also will pose similar challenges.** Today, this information lies

only with the network providers — which never shared with any application providers for the same reasons as discussed above.

Therefore it is not practically possible to selectively block applications at the OTT player level. However, one question still remains — **Can the OTT players block users using their IP addresses?** They can, provided they accurately get access to the user's IP addresses in the targeted geography. But how will they? And what purpose it will serve if someone is using VPN (proxy server) to camouflage his IP address? Using VPN and proxy servers the miscreants will find ways to circumvent the blocking and will end up harming only those users for whom the strategy was devised in the first place.

Selective Blocking (Network level) :

At the network level blocking can be done using the destination IP addresses of all the servers used by the OTT player. Note — the OTT players might have many servers, and some with the purpose of driving redundancy and efficiency. Adopting this strategy, the telecom operator will face many challenges.

Firstly, no OTT player will like to share his IP addresses to prevent hacking and denial of service attacks.

Secondly, the destination IP addresses of the OTT servers are dynamically changed to prevent tracing (by hackers).

Thirdly, even if these IP addresses are accessed in real-time through URL mapping (by physically checking each and every URL where they are heading), **it will still be a significant challenge for telecom operators to use them for the purpose**

of blocking. Why? The operators have to investigate each and every packet (originating from the BTS clusters) by doing a deep packet inspection — to identify those who they intend to block.

But how come some Chinese apps got blocked by the GOI? Did it not pose similar challenges? No. **To block these Chinses apps there was no need to do any deep packet investigation (DPI),** as they fall in the category of "simple blocking" and not "selective blocking". Just block the routing of traffic from India into those selected URLs and you are done. It is as simple as this. But if they show up again using a different URL then you have to identify them and block them as well.

Selective Blocking (5G Standalone)

The advent of 5G opens up some new possibilities. 5G standalone (not NSA), has the capability to dynamically set

routing of various applications at the device level using a feature called URSP (UE route selection policy). **Using this feature the network operator can decide the routing policy of data traffic emanating at the applications level from the user handsets.** The purpose of this feature is to distribute traffic within the network with the intent to drive efficiency and reduce latency. Now this feature only works in 5G handsets and that too in Standalone networks. With only one SA operator here coupled with limited 5G devices on the ground.

Q11. Whether there is a need to put in place a regulatory framework for selective banning of OTT services under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 or any other law, in force? Please provide a detailed response with justification.

Comments : Yes. Mentioned above.

Self regulation is failed.

With the aim to provide a regulatory code for video streaming platforms, the Internet and Mobile Association of India (IAMA) released a document called “Code of best practices for online curated content providers.”

- OTT platforms such as Netflix, Hotstar, Voot, Zee5, Arre, SonyLIV, ALT Balaji and Eros Now have signed the code, while Amazon Prime, TVF Play, Yupp TV, Hungama Play were missing from the list of signatories.
- The document aims to provide a guiding principle for Online Curated Content Providers, and outlines the kind of content that should be prohibited on video streaming platforms.
- It also calls for the setting up of a grievance redressal mechanism to ensure compliance of the code, and address complaints by the consumers.

- This should be seen in the backdrop of a discussion by the Observer Research Foundation held in September 2018, when some of the participating Video-on-Demand companies held that they should create a self-regulatory code for content before the government does.
- The code puts a responsibility on the signatories of this code against putting certain kind of content on their platforms.
- The nature of content covered is as follows:
  - Content which disrespects the national emblem or national flag.
  - Representing a child engaged in real or simulated activities or any representation of the sexual parts of a child for sexual purposes.

- Content which deliberately and maliciously promotes or encourages terrorism and other forms of violence against the State or its institutions.
- Content that has been banned for exhibition or distribution by online video service under applicable laws or by any court with competent jurisdiction.
- Transparent disclosure about the nature of content.
- The code also puts an onus on the video streaming platforms to inform the viewer about the nature of content.

➢ **What it does not cover:**

- The code does not specify the penalty or punishment to the grievance redressal department if it does not respond to the complainant within the specified period.
- It also does not specify the qualifications of a person who would be deemed fit to be a part of the grievance redressal department.

- The code does not give any power to the department to ensure the compliance of code.

The IT Act and the rules framed under it place certain regulatory obligations on body corporates or intermediaries which includes Telecom Service Providers (TSPs) and OTT services that can be regarded as same/similar to the services provides by TSPs. They are as follows:

➢ Lawful Interception obligations

➢ Takedown obligations

➢ Privacy and cyber security obligation

➢ Encryption obligations

Q12. In case it is decided to put in place a regulatory framework for selective banning of OTT services in the country, -

(a) Which class(es) of OTT services should be covered under selective banning of OTT services? Please provide a detailed response with justification and illustrations.

Comments :

Indians On Censorship :

1. As per a survey by YouGov, 57% of people (1005, approximately.), support partial censorship for online streaming. They think that a lot of offensive content i.e., unsuitable for public viewing is put up on such platforms. Majority of the people supporting censorship are adults of the age above 40s. However, the strongest arguments against such censorship is that the content on OTT platforms are Subscription on Demand, where viewers have choice to pay and select what to watch. Apart from this, the piracy of movies is another factor why filmmakers take the route of OTT. There are a large number of artists who don't have enough money to

portray their creative thoughts through cinema, OTT comes as a great breakthrough for them.

2. Perhaps it provides a worthy pedestal to build gripping story lines. And this is the reason why most of the viewers get attracted to the content provided by such platforms. They are fearless of the involvement of political parties and hence stream bold narratives and plots. They portray various socio-political issues which due to one or the other reason is not included in mainstream cinema.

3. And even after censorship in cinema, time and gain there have been huge disputes with regard to various movies like Padmavat, PK, My Name is Khan, etc. So there exists no reason that after censorship on OTT platforms, the content will not face any opposition. Also the content available on such platforms are affordable, belongs to the native language, deals with regional

content, provides free-trial facilities to users and most importantly is convenient.

4. Fake news is more dangerous than paid news and there is need to combat it jointly.
5. Determined to be detrimental to the national security, sovereignty and integrity of India
5. Promote Terrorism or instigates violence against state
7. Disrespect the National emblem or flag
8. Hurts any religious sentiments
9. Unnecessarily shows children engaged in sexual activity Politically sensitive contents etc.
10. **International Perspective** :

(i) Countries like Singapore, UK have regulatory bodies to keep a check on the OTT platforms. In Singapore, the service providers have to display the elements such as nudity, drugs, sex, violence, etc. in the content.

(ii) However, in UK, the OTT platforms face the same scrutiny as any public service broadcaster.

(iii) Australia has a principal legislation BSA, 1992 that governs the OTT sector.

(iv) While in Turkey, there is a licensing regime under which the OTT platforms are given a license for 10 years. Countries like Indonesia, Turkey and Saudi Arabia have strict regulations. They want total control in the hands of Government. Many OTT platforms including Netflix has been blocked.

(b) What should be the provisions and mechanism for such a regulatory framework? Kindly provide a detailed response with justification.

Comments : Mentioned Above.

Q13. Whether there is a need to selectively ban specific websites apart from OTT services to meet the purposes?

If yes, which class(es) of websites should be included for this purpose? Kindly provide a detailed response with justification.

Comments : Yes.

Following Websites can be prohibited :

1. Websites used for bypassing blocked content: These include proxy servers and virtual private networks (VPNs) that allow access to prohibited content.
2. Pornography, nudity and vice
3. Impersonation, fraud and phishing
4. Insult, slander and defamation
5. Invasion of privacy
6. Offences against the India and public order
7. Supporting criminal acts and skills: Content that provokes, calls for, promotes or provides information about how to carry out acts of crime or felony.

8. Drugs Addiction related

9. Medical and pharmaceutical practices that violate the law: This includes content used in promoting or trading pharmaceuticals without prescription.

10. Infringement of intellectual property rights

11. Discrimination, racism and contempt of religion

12. Viruses and malicious programmes

13. Promotion of or trading in prohibited commodities and services

14. Illegal communication services

15. Gambling

16. Terrorism

17. Illegal activities

Q14. Are there any other relevant issues or suggestions related to regulatory mechanism for OTT

communication services, and selective banning of OTT services? Please provide a detailed explanation and justification for any such concerns or suggestions.

Comments :

In China, local sites such as Tencent Video have accepted the terms of regulation imposed by the Chinese National Radio and Television Administration while the larger players such as Netflix and Amazon Prime remain banned. This is similar to the Chinese model of regulation of encryption where players such as Telegram and WhatsApp are banned, while local agencies such as We Chat remain in business after a substantial compromise on citizens' privacy.

In sum, while OTT regulation is desirable, the TRAI needs to accede to a higher standard of regulation than that of Singapore and China, one which is in line with its own constitutional values promoting online speech and creative freedom.

Registration:

We recommend that all OTT apps desirous of providing their services in India and all operating systems (Android, iOS, Windows, etc.) should be mandatorily registered in India and should be easily accessible by the government. Operating systems and apps come in varied forms, and with various tweaks and updates for various devices. Keeping track of all operating systems and apps would be a futile exercise, especially as open source apps and operating systems can be modified and re-deployed by anyone.

Thanks.

Yours faithfully,

(Dr. Kashyapnath)
President
Member Organization : TRAI