From: KMcAuliffe@itic.org
To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>
Cc: kdeep@itic.org
Sent: Friday, August 18, 2023 3:28:54 AM
Subject: ITI Response RE: Consultation Paper on Regulatory Mechanism for Over-the-top (OTT) Communication Services, and Selective Banning of OTT Services

Dear Shri Akhilesh Kumar Trivedi,

Please find attached the Information Technology Industry Council's Recommendations and Feedback on the Consultation Paper entitled "Regulatory Mechanism for Over-the-top (OTT) Communication Services, and Selective Banning of OTT Services." We appreciate the opportunity to provide feedback on this matter and would be happy to engage with you further.

Kind Regards,

Katie McAuliffe
Senior Director, Telecommunications Policy
Information Technology Industry Council

Please excuse typos; sent using dictation.

ITI Promoting Innovation Worldwide

August 18, 2023

To,
Shri Akhilesh Kumar Trivedi,
Advisor – Network, Spectrum & Licensing,
Telecom Regulatory Authority of India,
New Delhi, India

ITI Recommendations and Feedback on the Consultation Paper titled "Regulatory Mechanism for Over-the-top (OTT) Communication Services, and Selective Banning of OTT Services

The Information Technology Industry Council (ITI) is the premier global advocate and thought leader for the information and communications technology industry. ITI's membership comprises leading technology and innovation companies from all corners of the tech sector, including software, digital services, and internet companies. They are headquartered across Asia, the United States, and Europe, and many are significant investors and employers in India. On behalf of the global information technology sector, we are writing you to share our feedback on the Telecom Regulatory Authority of India (TRAI) released a consultation paper titled Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services ("Consultation"). ITI appreciates the opportunity to participate in this consultation.

A. Issues related to a regulatory mechanism for OTT Communication services

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

The time-tested distinction between infrastructure services such as broadband and spectrum controlling entities and application layer companies should be maintained in practice and in law, which is the basis of allowing innovation, international competition and deeper penetration and adoption of the internet in India. At the outset, any definition of telecommunication services should not include "application layer" components such as OTT services, as well as other internet-based communication services, interpersonal communications services, cloud service providers, etc. It is crucial to recognize that the current framework has played a significant role in fostering innovation in the technology sector, and that regulatory convergence that treats OTT services and TSPs similarly through regulation would prove counterproductive.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

OTT services is a term that should not be used in the context of India's regulatory framework. As TRAI has previously stated in its November 2018 Consultation, "there is no globally accepted definition of OTT services." (Consultation at para. 2.1.1) The term can mean many different things to many different people, resulting in uncertainty for both the regulator and entities potentially subject to regulation. Use of broad, unmanageable terms – such as "OTT" – in India's regulatory framework will create uncertainty, and this uncertainty will inadvertently impact the development of innovation from within India.

One, a clear classification of Over-the-Top services is often difficult due to the overlapping and dynamic nature of applications which provide more than one type of service. The same application may be providing person-to-person (P2P) communication, broadcast features, as well as curated content for entertainment. In fact, in various cases, P2P communication may only be a tertiary element of the platform, for a different service or objective. For example, e-commerce platforms, ed-tech platforms, and online gaming platforms all offer chat features to enhance user experience or provide customer grievance redressal. As such, these applications would already be regulated under the IT Act, 2000 and the IT Rules, 2021. Further, even though the application may satisfy the prescribed conditions to be classified as an OTT Communication Service, any new regulations which are imposed based on this premise are likely to affect the application's overall operations, and have unintended consequences for the business' ability to innovate, its ability to invest across Indian ecosystems, and the users' digital/fundamental rights like their right to receive and impart information online. For instance, additional requirements, on top of the IT Rules, around registration with a government authority, user verification, etc. will affect applications even though P2P communication may be a tertiary service they provide.

Two, any classification today is likely to become dated, as technology, products and consumer preferences evolve. It is difficult to foresee the direction of technological change, and any strict classifications and regulations targeting OTT Communication Services will inhibit the flexibility for innovation that tech companies require. For instance, the potential cost of regulations will make it difficult for companies to embed communication features which enhance the quality of their services and very often are geared towards (a) better experiences; and (b) ensuring consumer trust. Such classification will also create scope for regulatory arbitrage since companies will be burdened with two potentially overlapping and conflicting frameworks. Thus, it is better for India's ICT regulatory framework to adopt a rationalized approach which promotes dynamic innovation. Rigid definitions will ultimately rob India's digital economy of that dynamism and mitigate efforts to drive the Indian economy towards becoming a USD 10 trillion proposition.

ITI recognizes that there are many services operating "over-the-top" at the "application layer" of the internet. There is a diverse and wide range of digital services that use public internet for various consumer and enterprise-level application purposes. It would be a grossly unjustified simplification to term all of these as Over-the-top (OTT) services. Further, the technical, functional, and market-based distinctions between Telecom Service Providers (TSPs) and OTT/digital service providers must be emphasized. Traditional telecommunication services interconnect with the PSTN and provide crucial telecommunication infrastructure while

application layer service providers (such as OTT service providers) offer applications over telecommunications infrastructure. This distinction has long been acknowledged by TRAI in its recommendations regarding OTT communication services and should be maintained.

The vast majority of online services, sometimes referred to as 'OTT services', are in addition to, and not in derogation or substitution of, traditional telecommunications (or broadcasting) services.

OTT service providers cannot be considered as substitutes for TSPs as they are subject to different regulatory considerations and lack the same infrastructure rights and benefits. For example, compared to telecommunications, the OTT sector has vastly different competition and consumer protection considerations. The same application may be providing person-to-person (P2P) communication, broadcast features, as well as curated content for entertainment. In fact, in various cases, P2P communication may only be a tertiary element of the platform, for a different service or objective. For example, e-commerce platforms, ed-tech platforms, and online gaming platforms all offer chat features to enhance user experience or provide customer grievance redressal. As such, these applications would already be regulated under the IT Act, 2000 and the IT Rules, 2021. Further, even though the application may satisfy the prescribed conditions to be classified as an OTT Communication Service, any new regulations which are imposed based on this premise are likely to affect the application's overall operations, and have unintended consequences for the business' ability to innovate, its ability to invest across Indian ecosystems, and the users' digital/fundamental rights like their right to receive and impart information online.

While adoption of online communications by users is already considerable, that does not imply product market substitution, and certainly not complete substitution for traditional telephony, or for mobile networks. Users of these products also typically subscribe to traditional fixed and mobile services and use each of them as the circumstances and call types vary, depending on the use case (e.g., at home, on the road, personal use, professional use, intended call duration, combination with text, video and file transfer, unified communications, conference calls, business solutions, etc.). Usage is therefore more complementary and accretive than substitutive.

Therefore, the principle of 'same service, same rules' is misleading as these services may appear similar, but their infrastructure and delivery methods are fundamentally different.

To safeguard the future of data innovation, telecoms and applications must remain unbundled from a regulatory lens. Telecom law should regulate the hard infrastructure or 'carriage' layer, and not the layers above, such as software and applications. We would stress that this applies to all of the application layer services including but not limited to: OTT communication services and video services, machine-to-machine communication, and AR/VR communication and applications.

In terms of defining OTT services, in light of the above discussion, it can be said that the common criteria among varied OTT services is that they are provided to users over the public internet, or over the top of an existing network infrastructure. Any digital service will require at least a basic network infrastructure layer between the provider and the consumer. By that criterion, calling all digital services as OTT service will lead to erroneous and impractical conclusions. Hence, it is impractical to conclusively define OTT services.

Any classification today is likely to become dated, as technology, products and consumer preferences evolve. It is difficult to foresee the direction of technological change, and any strict classifications and regulations targeting OTT Communication Services will inhibit the flexibility for innovation that tech companies require. For instance, the potential cost of regulations, will make it difficult for companies to embed communication features which enhance the quality of their services and very often are geared towards (a) better experiences; and (b) ensuring consumer trust.

Lastly, we take this opportunity to note that OTT services all operate at the application layer; however, the OTT applications they provide vary greatly and, in that way, may warrant varied regulatory treatment that considers not only their status as OTT services or platforms, but also their distinct services, business models and customers. Any potential regulation should be risk-based and targeted to addressing specific identified harms or other concerns, focusing on a company's conduct, its business models, and its interaction, or lack thereof with end users. While certain rules may only apply to a narrow set of companies, it is essential that regulations be based on objective criteria, with proportionate, well-justified obligations accompanied by appropriate due process guarantees. Notably, such a system is already followed in India wherein the IT Act (defined below) read with Part 2 of the IL Rules (defined below) govern OTT communication services, Part 3 of the IL Rules governs video-based OTT platforms and digital news outlets, and the Consumer Protection Act, 2019 read with the relevant rules govern e-commerce entities.

2. **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.**

Application layer service providers offer applications within the application / software layer that is delivered over telecommunications infrastructure including: OTT communication services and video services, cloud computing, machine-to-machine communication, and AR/VR communication and applications.

Some of these application layer services are already regulated in India by the Information Technology Act, 2000 (IT Act) and the rules thereunder – such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data of Information) Rules, 2011 (SPDI Rules). Under the IT Rules, intermediaries – which are

likely to include most application layer service providers – are subject to dedicated compliance and reporting requirements. The introduction of a significantly broader and overlapping licensing regime under any telecom framework may qualify as an act of over-regulation on application layer services and also substantially increase compliance costs. This could hamper innovation and consumer choice. Furthermore, the Ministry of Electronics and Information Technology (MeITY) is in the process of developing a legal framework for the digital ecosystem under the Digital India Act (DIA)that is likely to be applicable to many application layer services, including OTT service providers.

Within OTT services, there are, for examples, OTT communication services and video services, and such OTT applications vary greatly and may warrant varied regulatory treatment that considers not only their status as OTTs, but also their distinct services, business models and customers.

Moreover, TRAI must consider the overlap in features that exist between various OTT services. Should TRAI seek to regulate only 'communication services,' (which is a sub-set of OTT services) it must also consider the practical limitations that such regulation may face and whether the regulation can be effectively administered. Even if a test is developed which seeks to differentiate communication OTT services from non- communication OTT services, such a test is likely to be flawed, as identifying whether the communication features are substantial or ancillary to the application may depend on vague and varying factors. In light of this, at this stage, it is not practicable to identify sub-categories of OTT services.

3. **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.**

As stated above, to safeguard the future of data innovation, telecom services and applications must remain unbundled from a regulatory lens. Telecom law should regulate the hard infrastructure or carriage layer, and not the layers above. We would stress that this applies to all of the application layer services including but not limited to: OTT communication services and video services, cloud computing, machine-to-machine communication, and AR/VR communication and applications.

Additionally, as noted by us above, the vast array of OTT services available can make it difficult to define. We note that OTT services all operate at the application layer; however, the OTT applications they provide vary greatly and, in that way, may warrant varied regulatory treatment that considers not only their status as OTT platforms, but also their distinct services, business models and customers. Any potential regulation should be risk-based and targeted to addressing specific identified harms or other concerns, focusing on a company's conduct, its business models, and its interaction, or lack thereof with end users. While certain rules may only apply to a narrow set of companies, it is essential that regulations be based on objective criteria, with

proportionate, well-justified obligations accompanied by appropriate due process guarantees. The existing legal framework in India already accounts for this aspect – as noted above.

For the same reasons the term "OTT services" should not be used in India's regulatory framework, ITI does not believe the term "OTT communications services" should be used in India's regulatory or licensing regime. The term does not establish service characteristics or capabilities that enable actionable decisions. See the answer to Q1 above.

At para. 2.39 of the Consultation, TRAI suggests that an "OTT service" is one that "is accessed and delivered through an application (App) over the public Internet, using the network infrastructure of telecom service providers; and…is a direct technical/ functional substitute for traditional telecommunication services provided by the telecom service providers." This definition provides no relevant or actionable criteria for determining whether or how a particular service should be regulated. The fact that a service is "delivered through an application (App) over the public internet" is so broad that it could include nearly everything happening on the internet. The second aspect of the definition – whether a service is a "direct technical/functional substitute for traditional telecommunication service" – provides no clarity or certainty as service providers will undoubtedly have very different views on what is or is not a substitute service.

We further reiterate from our response to question two, that TRAI must consider the overlap in features that exist between various OTT services, before attempting to define the same. Should TRAI seek to regulate only 'communication services' (which is a subset of OTT services) it must also consider the practical limitations that such regulation may face. Even if a test is developed which seeks to differentiate communication OTT services from non- communication OTT services, such a test is likely to be flawed, as identifying whether the communication features are substantial or ancillary to the application may depend on vague and varying factors.

That said, given the focus of this Consultation being on regulating OTT communication services, we have attempted to define the term based on the following features of OTT communication services – some of which we have already noted in our responses above:

At an operational level, OTT communication services fundamentally rely on services provided by TSPs (but the inverse is not true). Thus, TSPs hold the key to accessing internet services that are required by OTT communication services to allow them to function. Additionally, TSPs also hold the key that allows users to access OTT communication services, because without first purchasing internet access from TSPs they cannot access such services. Given the dependence of OTT communication services on the network infrastructure provided by TSPs, they cannot be considered substitutable services. Additionally, at a technical level, TSPs, through their network operations, have the rights to use and monetise critical resources on which the application layer is dependent. To elaborate, TSPs control the underlying infrastructure, in addition to which they have the power to acquire spectrum, interconnect with the PSTN, build network infrastructure, etc. On the other hand, OTT service providers are entirely dependent on the decisions TSPs make in deploying infrastructure and providing internet access. These differences have been

acknowledged in foreign jurisdictions as well. For example, Australian Competition and Consumer Commission, in its Communications Sector Market Study (April 2018), noted that OTT services and traditional voice services ought to not be regulated similarly – given that they, at this stage, are not complete substitutes for one another.

4. 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.

Please refer to ITI's response to Question 2 above.

5. Please provide your views on the following aspects of OTT communication services vis-à-vis licensed telecommunication services in India:
   (a) regulatory aspects;
   (b) economic aspects;
   (c) security aspects;
   (d) privacy aspects;
   (e) safety aspects;
   (f) quality of service aspects;
   (g) consumer grievance redressal aspects; and
   (h) any other aspects (please specify).

   Kindly provide a detailed response with justification.

Application layer services and network layer services can be offered with distinct requirements and obligations relating to the matters discussed above, noting that some categories (such as quality of service) are only appropriate for layers that control network facilities. Notwithstanding those distinctions, enterprises and consumers experience and interact through the ecosystem at both application and network layers, and both layers are important. Today's digital marketplace consists of many building blocks, including network infrastructure such as telco and ISP networks, internet exchanges, enterprise networks, subsea cables, and satellite networks, as well as cloud infrastructure such as data centers, edge-computing nodes, and content caches.

ITI recognizes that both the network service provider (NSPs, such as telcos and ISPs) segment and cloud service provider (CSPs, and/or digital platforms) segment have made multi-billion-dollar investments annually in building and sustaining a global digital infrastructure in the past decade. Telco network infrastructure investments and cloud infrastructure investments are complementary and increasingly convergent. Both sets of investments are critical to India's digital infrastructure goals. Each segment needs to grow and sustain its investments independently for a greater total investment in India's digital infrastructure.

As TRAI inherently recognizes in light of this question regarding both TSPs and OTTs, the internet is much more than a TSP's last mile connection; rather it is a complex, interdependent

ecosystem. The underlying infrastructure enabling digital transformation involves many building blocks and many investors. While telco last-mile networks are important parts of the modern internet infrastructure, they are not in its entirety. A diverse ecosystem of many industry participants contributes to the building blocks of the modern internet.

Below, we have commented on various laws and regulations that deal with each of the aforementioned aspects, and the initiatives taken by OTT communication services under each aspect. We have also commented on how TSPs have economically benefitted from OTT communication services.

(a) Regulatory aspects:

TSPs have long demanded a 'level-playing field' with respect to regulation of OTT communication services. They place reliance on the 'same service, same rules' principle, however, this fails to account for the fundamental differences between the two types of services. Thus, to account for their differences, TSPs and OTTs should not be regulated under the same regime.

As explained in the response to Questions 1 and 3, TSPs and OTT service providers operate on different layers of the internet. TSPs control and operate the underlying network infrastructure that provides access to the internet, and OTT service providers are entirely dependent on this internet access to provide their services and content to end-users. Further, the markets within which TSPs and OTT services operate are different. TSPs control the access to over a billion consumers in India and are thus subject to stringent regulatory and licensing framework because they are entitled to certain rights that OTT service providers do not enjoy.

Licensing in the telecom context is premised on the limited number of operators in the market and the scarce, rivalrous and excludable nature of spectrum resources, which necessitates government intervention to achieve public welfare goals. On the other hand, OTT services are plentiful and internet users can switch between OTT services easily. The same user may be using one or more OTT services as she prefers. In light of this, the rationale for telecom licensing is patently inapplicable to the OTT services context. Further, the distinction between licensing for the network layer, provided by the TSPs, and the application layer, provided by OTT Services, is important. While the former is under the jurisdiction of the Ministry of Communications, the latter is under the Ministry of Electronics & Information Technology.

Additionally, OTT communication services have been typically regulated under a different set of laws, such as the IT Act and the rules and regulations issued thereunder, including the IT Rules and SPDI Rules. Beyond the existing legislation that govern OTT communication services, they may also be regulated under the upcoming Digital Personal Data Protection Bill, 2023 (DPDP Bill), and - based on public statements made by the Central Government - the DIA.

(b) Economic aspects:

Certain industry stakeholders are of the view that OTT service providers free ride over the infrastructure established by TSPs. They argue that OTT service providers ought to compensate TSPs for expenses incurred in establishing, operating, and maintaining the underlying infrastructure. However, OTT service providers do not free ride since they make significant contributions to the revenue generated by TSPs. These contributions are the combined effect of the rise in the digital economy, an increase in demand for online content / services, and also an increase in demand for internet access needed to access OTT services. OTT communication services have in essence created a new source of revenue for TSPs through the rise in demand for such services.

The growth in TSPs' revenue is evidenced by: (i) the monthly average revenue per user for wireless services increasing 44% from 2012 to 2022; (ii) the growth in volume of monthly wireless data usage increasing by about 156 times from 2014 to 2022; and (iii) the average revenue from data usage per wireless subscriber per month increasing about 5.6 times from 2014 to 2022. These statistics – as cited by the TRAI in the Consultation - support the finding that there is no evidence to justify a mechanism where OTT providers compensate TSPs for costs incurred in establishing and maintaining their network infrastructure. Based on such lack of evidence, the BEREC had similarly noted in its 'Preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs' (October 2022) that we cannot justify the implementation of a direct compensation mechanism, which resembles the 'SPNP' principle. In fact, the Broadband India Forum's report on the Economic Value of the App Economy in India (2023) supports the theory that besides the direct effect of the app economy (a large portion of which we assume is sustained by OTT platforms) on the GDP, there are indirect effects in supply industries as well – including the telecom sector. Therefore, OTT services, specifically OTT communication services, have an overall positive impact on the Indian economy, including the revenues earned by TSPs.

(c) Security aspects:

The IT Act already imposes several safety and security obligations on OTT communication services to ensure user safety online and in the interests of cyber-security. As such, no further regulation is required to deal with the security offered by OTT communication services, or in the interests of cyber-security.

The Indian Computer Emergency Response Team (CERT-In) deals with cyber security in India. The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules) broadly prescribe compliances on cyber security (such as incident reporting, appointing a point of contact, etc.) to a wide range of entities, including OTT service providers. This is complemented by the April 2022 directions issued by the CERT-In under Section 70B(6) of the IT Act relating to 'Information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

Further, under Section 43A of the IT Act, any 'body corporate' handling sensitive personal data or information (SPDI) will be liable to pay compensation to affected persons if it fails to implement adequate security practices and procedures and causes wrongful loss or wrongful gain to any person. These reasonable practices are prescribed in detail under the SPDI Rules. The SPDI Rules also stipulate additional data privacy related obligations that OTT service providers have to comply with. Moreover, once the DPDP Bill is enacted, there will likely be even more stringent obligations on OTT service providers to implement reasonable security safeguards in order to prevent data breaches.

The IT Act also empower the Government to, in the interest of national security, public order, etc., issue directions under: (i) Section 69 for interception, monitoring, and decryption; and (ii) Section 69A for blocking unlawful content in any computer resource. Additionally, under Section 69B the Government can issue directions to monitor and collect traffic data or information for cyber-security purposes.

(d) Privacy aspects:

As noted above, the SPDI Rules regulate OTT service providers in matters pertaining to the processing of personal information (PI) and SPDI. Flowing from this regulation, OTT service providers have specific privacy related compliances under the SPDI Rules. Notably, OTT service providers are required to provide a privacy policy for PI or SPDI being processed, obtain informed consent for the collection and use of SPDI, adhere to third-party disclosure and transfer requirements, etc. Once the upcoming DPDP Bill is enacted, the privacy obligations on OTT service providers will become even more rigorous.

(e) Safety aspects:

OTT communication services comply with the cyber-security and data privacy obligations under existing laws like the CERT-In framework and the SPDI Rules – as noted above. In addition to this, they are undertaking their own internal measures to provide a safe and secure experience for their users. For example, many OTT communication services have safety features like a two-step verification process, the option to block other user accounts and report content, and the ability to implement various other privacy controls. OTT communication services have also been working to introduce additional security features in response to issues arising from the circulation of spam and fake news on their platforms. This includes notifying a user when a particular message has been forwarded multiple times, or adding labels to information that may be false or inaccurate. Beyond their own initiatives, certain OTT communication services currently also cooperate with law enforcement authorities and the Government (such as the DoT) to block accounts of users who have obtained numbers using fraudulent means.[1]

[1] For example, WhatsApp to axe numbers flagged fraud on DoT's portal, available at https://economictimes.indiatimes.com/tech/technology/whatsapp-to-axe-numbers-flagged-fraud-on-dots-portal/articleshow/100285792.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

Additionally, as per news reports, it is likely that online safety and trust will be one of the important aspects addressed in the DIA. As part of this, OTT communication services governed by this law may be required to adopt additional safety features as well.

(f) Quality of service aspects:

Strong competition in the OTT services market means that OTT services are incentivized to maintain a high quality of service to stand out from their competitors, and not just attract more users but also retain their existing ones. Retention of users is critical because of the ease with which users can switch from one OTT communication service to another, and the various options available to choose from.

Therefore, there is no need to subject OTT service providers to stringent quality of service benchmarks, as this may inhibit their ability to constantly innovate and create new features or offerings for their users. It is also likely that the imposition of quality-of-service benchmarks will lead to an increase in operational costs.

(g) Consumer grievance redressal aspects:

Certain OTT communication services are governed by grievance redressal requirements under existing laws. For example, paid online services are subject to such requirements under Consumer Protection Act, 2019; and OTT communication services (acting as intermediaries) are subject to the same under the IT Rules.

Under the IT Rules, intermediaries are required to set up a grievance redressal mechanism, publish the contact information of the grievance officer and redress complaints within specified timelines. Thus, OTT communication services are currently subject to sufficient regulations vis-à-vis grievance redressal.

6. **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.**

Creating a licensing regime for services delivered via the internet that is converged with or mirrors licensing regimes for telecommunication service providers would cause considerable disruption to India's ICT industry. As explained earlier, many application layer services (such as OTT communication services) are already regulated in India by the Information Technology Act, 2000 (IT Act) and the rules thereunder – such as the IT Rules and the SPDI Rules. Under the IT Rules, intermediaries – which are likely to include most application layer / OTT service providers – are also subject to dedicated compliance and reporting requirements.

Furthermore, each administrative establishment, under each Ministry of the Government, has a unique mandate and purpose. For context, DoT deals with issues relating to communications which include voice, video, and data communication, while MIB deals with information and broadcasting technologies; the Ministry of Electronics and Information Technology (MeitY) considers issues related to electronics and information technology. Together, they form a comprehensive regulatory ecosystem for the carriage of online, telecom and broadcasting services in India. Furthermore, MeitY is in the process of developing a legal framework (i.e., the DIA) for the digital ecosystem that is likely to be applicable to many application layer services, including OTT service providers.

Further, we would emphasize key differences between TSPs and application layer services (such as OTT communications services). TSPs receive exclusive rights and privileges from the Government, such as right to acquire spectrum, right of way, etc. and they own and control what is considered critical infrastructure in India. Thus, a licensing regime on traditional telecommunication service providers is justified to ensure their accountability. On the other hand, OTT services do not acquire and deploy scarce resources (such as spectrum) or typically use government resources (such as telephone numbers), and they have no actual control over the networks that do. The imposition of heavy financial obligations, designed to protect the public's interest in licensees' use of these resources, is unnecessary and likely to reduce OTTs' ability to invest in improving the quality of their services. Moreover, it may also compel them to shift the burden of their increased operating costs onto the users (by making their services more expensive).

This would run contrary to TRAI's own observations in its 2020 recommendations on "Regulatory Framework for Over-The-Top (OTT) Communication Services". TRAI observed that a comprehensive regulatory framework for OTT services is not recommended beyond the existing laws and regulations. It was of the opinion that such regulation could be looked into afresh when more clarity emerges in international jurisdictions, "particularly the study undertaken by the ITU." Between 2020 and 2023, there has been no change to this situation vis-à-vis international practices; and also, no change in ITU's approach. In fact, ITU has not specified any regulatory mechanism for OTT based services and has only encouraged voluntary commercial agreements between TSPs and OTT service providers. Additionally, TRAI in 2020 also recommended that no regulatory interventions are required in respect of issues related with privacy and security of OTT services.

Thus, OTT services should not be regulated under a similar framework as telecommunication service providers as their accountability cannot be equated and it is likely to negatively impact application layer services as well as their end users.

In our view, licensing is usually required where resources are scarce and operators obtain something of value in turn for a license, such as spectrum (for mobile, television, or radio channels), or when the licensee is given the right to use telephone numbers or rights-of-way. When it comes to online services, there is a virtually infinite number of services that can be

offered which do not require the allocation of such finite resources. As such, we do not believe that a licensing regime is appropriate for online applications and services, especially OTT communication services.

Thus, the regulation of OTT services and other application layer service providers should be left to be carried out under the IT Act and existing frameworks itself. Any permission-based regime (such as in the form of licenses) should only extend to those services with access to resources, which traditionally qualify as 'material resources' and are under the ownership of the government, such as spectrum assignment. Bringing internet communication services within the regulatory ambit of DoT or another regulator would not only subject such services to onerous license terms and conditions, but would also include a levy of entry fees, license fees and registration fees. This will have a downward pull on innovations and investments in the internet and digital ecosystems in India.

Lastly, we would like to point out licensing would also have other negative impacts for innovation and investment in the internet ecosystem. To elaborate, the market for OTT communication services is characterized by low barriers to entry, and constant innovation that sets such services apart from their competition and helps them add value to their services. Imposing onerous regulatory obligations intended for traditional telecom sector services on OTT communication services (which are typically offered for free) will not only affect the ease of doing business but will also reduce the ability of OTT service providers to invest in technology and service innovation. Additionally, subjecting OTT communication services to a licensing framework meant for TSPs may create an uneven playing field between service providers that provide communication services and those that do not (in addition to the fact that there is no bright-line test to determine when a service is communication based and non-communication based – as noted by us in our responses above). In such a scenario, it is entirely possible that OTT service providers may reduce investments in communication services and instead focus on developing and investing in 'non-communication' services.

Therefore, the introduction of a significantly broader licensing regime (or any other new regulatory framework) may qualify as an act of over-regulation on OTT communication services operating on the application layer services and substantially increase compliance costs. This could hamper innovation and consumer choice, create confusion for operators and the internet and digital ecosystem and reduce ease of doing business, despite the well-intentioned aim of the government.

7. 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:
    (a) lawful interception;

(b) privacy and security;
(c) emergency services;
(d) unsolicited commercial communication;
(e) customer verification;
(f) quality of service;
(g) consumer grievance redressal;
(h) eligibility conditions;
(i) financial conditions (such as application processing fee, entry fee, license fee, bank guarantees etc.); and
(j) any other aspects (please specify).

ITI suggests no licensing or regulatory framework for OTT communication services as they are already regulated by different government departments through existing and upcoming legislation. OTT applications vary greatly, and warrant varied and targeted regulatory treatment that considers not only their status as OTTs, but also their distinct services, business models and customers.

Separately, we would like to take this opportunity to reiterate the fact that there is currently an extensive legal regime that governs various OTT services. We have elaborated on this below.

(a) Lawful interception:

Sections 69, 69A, and 69B of the IT Act empower the State to, respectively: (i) intercept, monitor, and decrypt information generated, transmitted, received or stored in a computer resource; (ii) block public access to information any computer resource; and (iii) monitor and collect traffic data or information in a computer resource. Please refer to the response to Question 5 for more details.

(b) Privacy and security:

The CERT-In framework and the SPDI Rules contain obligations that deal with cyber-security incidents and protect the PI or SPDI of individuals. Please refer to the response to Question 5 for more details.

(c) Emergency services:

TSPs are required to provide public utility / emergency services under the existing Unified License framework. Such services include toll-free services for police, fire, and ambulance purposes. The idea behind this is to ensure subscribers are not charged for making calls during an emergency or are prevented from making such calls in the event they, for instance, have insufficient funds.

OTT service providers should not be subject to such emergency requirements because of the specific circumstances under which they function. That is, OTT communication services need the internet to operate, and the internet may not always be available to a user during an emergency. Further, most OTT service providers do not connect to the PSTN or have the infrastructure or technical capability to provide emergency calling services – especially keeping in mind the nature of non-interconnected OTT communication services. In addition, to provide emergency services, especially with respect to search and rescue operations, ascertaining an individual's geo-location is important. However, any given OTT service provider may not have access to this location information depending on users' privacy settings on their platform.

(d) Unsolicited commercial communications:

OTT communication services have taken their own initiative to introduce features that allow users to report or block the senders of spam or unsolicited messages and calls. We believe that this is sufficient for the time being.

(e) Customer verification:

OTT communication services generally undertake verification of any user that signs up for their services, either through an OTP sent to a phone number or email. The IT Rules also mandate intermediaries such as significant social media intermediaries to enable users to voluntarily verify their accounts through appropriate mechanisms. Therefore, to this extent, OTT communication providers that fall within the definition of significant social media intermediaries are already subject to such requirements.

Additionally, we understand that certain OTT communication service providers have executed voluntary agreements with regulatory authorities – such as the DoT – to deal with instances where users with disconnected phone numbers continue to use their communication service, by undertaking a re-verification of such users / numbers.

(f) Quality of service:

Please refer to the response to Question 5 above on 'quality of service aspects'.

(g) Consumer grievance redressal:

Please refer to the response to Question 5 above on 'consumer grievance redressal aspects'.

(h) Eligibility conditions:

N/A, since we believe that there is no need to introduce any new licensing or regulatory framework for OTT communication providers.

(i) Financial conditions:

N/A, since we believe that there is no need to introduce any new licensing or regulatory framework for OTT communication providers.

8. **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.**

A collaborative relationship already exists between OTT service providers and TSPs – they exhibit a 'symbiotic relationship,' as the content provided by OTT service providers drives demand for network services and thus also benefits TSPs in increased data usage, thus driving up their revenues and getting more customers on board. There is no need to introduce a separate collaborative framework between OTT service providers and TSPs. As discussed above in our answer to Q5, there is much more to the internet than the last-mile networks of TSPs. While a critical component of providing innovative services to India users, the last mile is only one of many internet components requiring investment.

To facilitate appropriate public policy decisions that will benefit consumers and businesses in India, TRAI should consider the following recommendations:

- Keep in view the entirety of the digital infrastructure, not just the telecom last-mile networks, which is discussed above in our answer to Q5.
- Recognize investments and contributions from all players along the internet value chain and incentivize sustained investments from each part of it.
- Reject the call for regulatory intervention in the absence of market failure.

To elaborate, OTT service providers invest in content, applications, and skills development, for example, which are all essential to meet India's connectivity goals and contribute to the Indian economy. Although OTT service providers invest primarily in their business products, they also significantly invest in R&D, content, and services, as well as complementary investments in infrastructure such as undersea cables, data centers etc, within India.[2]

While incumbent TSPs are the primary investors in physical infrastructure (as they should be), if we are to consider the internet ecosystem as a whole, investment should be considered broadly as well. As pointed out by BEREC in its report on 'Preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs' (October 2022) and reiterated in BEREC's

[2] https://telecominfraproject.com/facebook-partnering-to-build-the-telecom-infra-project/ and https://cloud.google.com/blog/products/infrastructure/announcing-the-blue-and-raman-subsea-cable-systems

2023 Response to the Exploratory Consultation, the different roles of the players contributing to this ecosystem must be taken into account.[3]

Many technology companies offering OTT communication services invest heavily in network infrastructure, services, and products that support telecom operators' effective network management and reduce their costs. This includes large data centres for storing content closer to end users. Some OTT service providers also invest in subsea cables that connect global internet traffic and provide networks with high-speed content delivery, resilience, and capacity. That in turn benefits their retail customers.

Content Delivery Networks (CDNs), whether built by an OTT service / content provider or a third-party partner, are a layer in the internet infrastructure that pushes OTT services closer to consumers and alleviates the pressure on TSP infrastructure. In the event that a CDN does not have its own data centre close enough to the end-user, CDNs pay TSPs for hosting content on the TSP's servers. This improves the end user's experience by reducing latency and improving quality, while also providing a revenue stream for TSPs.

Another example is internet exchange points (including those operated by private entities) wherein they provide cost-effective critical infrastructure and points of interconnection for smaller content and applications providers to route their traffic within India and reach their consumers.

The October 2022 report by Analysys Mason on the 'Impact of tech companies' network investment on the economics of broadband ISPs' shows OTTs have invested almost USD 883 bn in digital / internet infrastructure globally from 2011 to 2021, averaging USD 120 bn annually in recent years and saving ISPs between USD 5 bn to USD 6.4 bn a year.[4]

This mutual interdependence, which is acknowledged in BEREC's 2022 preliminary assessment and BEREC's 2023 Response,[5] has delivered huge advantage to consumers and users who benefit from unfettered access to a rich ecosystem of online content, applications, and services. It also

[3] https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%20%2822%29%20137%20BEREC_preliminary-assessment-payments-CAPs-to-ISPs_0.pdf. This view was restated in BEREC's Response to the EU's 2023 Exploratory Consultation: https://www.berec.europa.eu/system/files/2023-05/BoR%20%2823%29%20131b%20Overview%20of%20BEREC%20Response%20to%20Exploratory%20Consultation.pdf

[4] https://www.analysysmason.com/consulting/reports/internet-content-application-providers-infrastructure-investment-2022/

[5] Preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs' (October 2022) BERC. https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%20%2822%29%20137%20BEREC_preliminary-assessment-payments-CAPs-to-ISPs_0.pdf. BEREC's Response to the EU's 2023 Exploratory Consultation: https://www.berec.europa.eu/system/files/2023-05/BoR%20%2823%29%20131b%20Overview%20of%20BEREC%20Response%20to%20Exploratory%20Consultation.pdf

brings about socio-economic benefits and access to entertainment and information that enriches consumers' lives as well as economic opportunities.

An analysis[6] by the Internet Freedom Foundation found that the telecom industry-wide average revenue per user (ARPU) has increased steadily between 2018 to 2023 in India. User engagement with OTT applications is directly proportional to the amount of data consumed over the internet. OTT applications encourage people to purchase data packs and upgrade to higher-tiered data services supplying faster speeds and greater bandwidth. In other words, OTT apps help telecom operators by boosting demand for data usage.

Regulating collaboration will harm India consumers and businesses because there is no market failure that needs to be addressed. The internet economy in India, and around the globe, continues to be a market success and key economic driver, not a market failure warranting regulatory manipulation. Each segment of the internet value chain sustains and evolves itself through healthy competition within the segment. Proposals of forced subsidy from one part of the value chain to another would disrupt well-functioning market growth and innovation and should not be imposed without objective demonstration of existing market failure. None has been demonstrated. In fact, the telecom sector has benefited from the growth of internet traffic; the growth in internet traffic is not a burden but rather it is the main driver for telecom revenue growth.

We believe that the Indian ecosystem should continue to encourage this kind of symbiotic relationship for the benefit of all actors in the ecosystem, beginning with end users, without any additional regulatory intervention.

9. **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.**

If by "collaborative framework," TRAI is considering the imposition of a network usage fees model, ITI notes that network usage fees would distort market incentives and give TSPs / ISPs disproportionate leverage over OTT service providers. To compel certain OTT service providers to pay network usage fees, an TSP / ISP could be disincentivised to address traffic congestion on its network or to optimise performance by design to the benefit of their customers, effectively restricting end users from receiving the requested service from OTT service providers at the quality the user desires (and thus impacting their welfare in the long-run). This congestion represents powerful leverage for a TSP / ISP to force OTT service providers to pay network usage fees. TSPs / ISPs may also be unwilling to accept co-investment and cost-saving measures offered by content providers that would increase service performance for end users, such as caching and peering, in order to receive maximum network usage fees, which would raise the cost of the

[6] https://internetfreedom.in/public-brief-on-fair-share/

internet for everyone. This would also mean that the routing for data packets ultimately would be decided based on economic reasons, i.e., to minimize traffic charges, rather than for the primary purpose of technical efficiency which so far, would normally direct the traffic to be delivered in a way that most appropriately serves quality of experience of users.

Moreover, historical data demonstrates that network usage fees are inefficient and increase the cost of service. The internet ecosystem has grown considerably and evolved rapidly in just two decades without mandatory inter-operator payments. Consumers benefit most when traffic is exchanged without payment. If there is no demonstrable market failure – and in this case, none has been shown – then regulatory intervention threatens to distort otherwise market-efficient outcomes, to the detriment of consumer welfare and achieving India's digital goals.
Mandatory payment regimes also create distortions, such as:

- *Administrative costs*. For example, cloud and telco operators understand that traffic exchange payments generate administrative costs for setting, calculating, and paying/collecting payments. They often decide that these administrative costs would outweigh the potential income they might generate and are not worth incurring.

- *Negative impact on consumers*. Mandatory traffic payments may end up being passed along to consumers and businesses in India, causing them to pay more for the identical combination of content and internet access service.

- *Negative impact on the growing Indian content industry*. Mandatory usage fee payments will increase the costs of distributing content on the internet and, if adopted in India, could be mimicked by other countries. In turn, it will dampen the global expansion and consumption of an otherwise dynamic Indian filmmaking and sports sector.

Further a revenue sharing model may violate the principle of net neutrality and oppose the open and free nature of the internet. For example, net neutrality may be violated if different network usage fees are charged to different OTT communication services, and larger OTT communication services are required to pay a higher share of the fees to TSPs. Additionally, net neutrality may be at jeopardy in cases where TSPs with their own OTT communication services may be exempt from any network usage fees requirement. This aspect would also raise competition law concerns.

Relationships between OTT service providers and TSPs / ISPs are already balanced (as highlighted in Question 8). Inserting a requirement for paid peering / revenue sharing / network usage fees (by whatever name such a system is called) into the market would override the current market-based approach of settlement-free peering and removes the possibility of other agreements and further innovation in traffic management. The most prevalent method of managing network traffic is through settlement free peering agreements. Any regulatory intervention in this regard would limit nearly all interconnection options to paid peering, thereby interfering with providers' ability to manage arrangements according to local needs and could result in lower quality of

service, inefficient traffic flows, higher data transmission costs and less resilient networks overall. Such an approach would upend the open internet architecture and fly in the face of net neutrality.

We note that these are concerns that domestic industry bodies, such as the Internet and Mobile Association of India, and think tanks, such as CUTS International, have recently raised in the Indian context as well, in light of revenue sharing demands posted by TSPs.[7]

B. Issues Related to Selective Banning of OTT Services

ITI recognizes that governments have legitimate needs to seek access to technology, as well as the data of commercial entities, including for law enforcement, intelligence, counterterrorism, or national security purposes. At the same time, it is important to recognize that promoting trust for the 'Digital Nagrik' is dependent upon protecting the fundamental values of openness, safety, security, and privacy. ITI continues to work with governments around the world in developing policies to enable legitimate government access – details of which can be found in our Global Guiding Principles for Trust, Technology and Government Access in the Digital Age.[8]

Furthermore, ITI recommends that any proposed rules pertaining to selective banning exclude subject categories such as OTT services provided by internet intermediaries that are already subject to the IT Act and IT Rules.

10. 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.

Before delving into the technical and regulatory aspects of selectively banning OTT services, it is crucial to examine the existing data on internet shutdowns in India. The 26th Report by the Parliament Standing Committee on Information and Technology (SCIT) revealed that there is no official record of internet shutdowns maintained by central or state governments. The SCIT expressed disappointment in the lack of effort by the Ministry of Home Affairs (MHA) and DoT to track shutdowns across the country. This absence of data hinders the understanding of whether shutdowns comply with the safeguards outlined in the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, and the Supreme Court's directions in Anuradha Bhasin v Union of India and Ghulam Nabi Azad vs Union of India. Public databases, however, indicate that India has experienced numerous shutdowns, with a significant proportion being employed for routine policing and administrative purposes, rather than being directly related to large-scale public safety concerns or emergencies. The Telecom Suspension Rules, established in 2017, grant the power of blocking to the Home Secretary at the central or state

[7] Please see https://cuts-ccier.org/ott-regulation-should-keep-consumer-interest-in-consideration-cuts-international/; https://economictimes.indiatimes.com/industry/telecom/telecom-news/revenue-share-underhanded-attempt-to-violate-net-neutrality-iamai-on-coais-demand-of-compensation-by-otts/articleshow/98169929.cms?from=mdr

[8] https://www.itic.org/dotAsset/8/0/80ec80e7-7898-42b0-95db-6c4d4a57e932.pdf

level, with the requirement of recording reasons for the shutdown in writing. A review committee assesses these orders periodically to ensure compliance with the rules and principles of proportionality. Prior to 2017, Section 144 of the Code of Criminal Procedure was used for shutdowns at the district level, but the Supreme Court ruled that all shutdown orders must be published and subject to judicial review. Nonetheless, publication of such orders is still not consistently followed, leaving uncertainty regarding their compliance with statutory, judicial, and constitutional safeguards.

Selective banning of websites / OTT services may be counterproductive because users will find ways to circumvent bans, such as through VPNs, or simply by switching to less popular and potentially less secure online services. There is evidence to suggest that when popular messaging services are banned in certain jurisdictions, users respond by switching to alternate options with ease. An example of this would be when Chinese users switched to Signal right after the U.S. Government announced a ban in 2020 on China's most popular messaging app. As an example, when Russia banned Facebook and Instagram in 2022, it has been publicly reported that the demand for VPNs increased substantially Thus, selective banning may not be the most effective strategy to counter terrorism or curb unrest within the country. Instead, it may adversely affect the users and local communities who wish to access OTT services for legitimate reasons.

To elaborate, small and medium businesses depend on OTT services to carry out their day-to-day functions. In this regard, it is important to note that the Supreme Court of India has – in Anuradha Bhasin v. Union of India & Ors., W.P. (C) No. 1031 of 2019 - held that fundamental rights such as the right to speech and expression under Article 19(1)(a), and the right to carry on trade, business, or occupation under Article 19(1)(g) of the Constitution of India, 1950, are protected even over the internet. Therefore, before blocking OTT services, any Government should ensure that, at the very least, the same is a proportionate response to the issue it is seeking to tackle. There is still a lack of clarity as to the efficacy of internet shutdowns in preserving public order, and whether selective banning is a better solution to total internet shutdown. We believe that blocking an entire OTT service is only a proportionate response if such OTT service has intentionally violated compliances under applicable laws in India. Indeed, this scenario is already covered by Section 69A of the IT Act.

Selective banning of websites / OTT services also raises privacy concerns and poses certain technical challenges.[9] To begin with, it is possible to selectively ban websites following the DNS (and having identifiable URLs / IP addresses). However, the likelihood of users trying to circumvent this type of selective banning cannot be ruled out. They may, for example, use VPNs to get past the bans.

In terms of selectively banning OTT services – the same can be pursued at the OTT application level or at the TSP level. At the application level, OTT service providers will require the location

[9] Selective banning of OTT Application', available at https://paragkar.substack.com/p/selective-banning-of-ott-application.

information of all users in order to block their services in a specific geographic area. Accessing such user information raises privacy concerns, particularly in light of the imminent DPDP Bill. Additionally, OTT service providers will have to take the consent of users to access their location information – not all users may be willing to share such data with OTT service providers.

At the TSP level, blocking can be done using the destination IP address of all the servers used by an OTT service provider. This process may also prove to be challenging because OTT service providers may be reluctant to share their IP addresses (for cyber-security reasons, etc.). Even if they do, the destination IP addresses of servers used by OTT providers are usually hosted on the cloud and, as such, tend to be dynamic. Further, there may be situations where various OTT services are hosted on the same cloud service and may be using the same dynamic IP address. In this regard, there is a possibility that some OTT services can be accidentally blocked by TSPs relying on such IP addresses. To avoid this scenario, TSPs may have to conduct a deep packet inspection. That is, if TSPs are able to access the IP addresses of OTT services by way of URL mapping, TSPs may have to investigate each packet of data being sent over the internet to ensure that they block the correct OTT service using such IP address. In addition to being an onerous exercise, this could have far-reaching privacy, free speech, and net neutrality concerns. Therefore, selective banning of OTT services is not a practicable approach. In any case, VPN services will continue to function as a workaround to the same.

11. 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.

The IT Act has adequate provisions that allow the blocking of online content. That is, provisions like Section 69A of the IT Act read with the Blocking Rules may be sufficiently relied on to block specific posts or an entire OTT platform or service. We understand that the Government has, in fact, invoked its powers under Section 69A in the recent past to block several OTT platforms in the interest of national security. Similarly, Section 79 of the IT Act read with the IT Rules allows the blocking of online content as well under certain grounds.

In light of the existing legal frameworks, there is no need for a new framework on the selective banning of OTT services, and the IT Act can continue to be relied upon. This will ensure a balance between the public's right to access an OTT service, an OTT service's ability to offer its platform to users, and the Government's interests in tackling unlawful or illegal activities.

12. 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.
    (b) What should be the provisions and mechanism for such a regulatory framework? Kindly provide a detailed response with justification.

N/A – since we believe there is no need to introduce a regulatory framework for selective banning of OTT services.

13. 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.

N/A – since we believe there is no need to introduce a regulatory framework for selective banning of websites.

14. 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.

N/A – we have provided all our concerns and comments on the issues considered by the TRAI, as part of this Consultation, in this document.