



Mr. Akhilesh Kumar Trivedi,  
Advisor (Networks, Spectrum and Licensing),  
Telecom Regulatory Authority of India (TRAI)  
New Delhi, India  
*Via electronic mail: advmn@traai.gov.in*

18 August 2023

**Re: Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services.**

To whom it may concern:

The Computer & Communications Industry Association (CCIA) submits the following comments regarding the Telecom Regulatory Authority of India (TRAI) “Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services.” CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms.<sup>1</sup>

CCIA appreciates the opportunity to provide its views in this consultation and supports TRAI for undertaking a detailed analysis of, and seeking stakeholder inputs on, the opportunities and – more specifically – the challenges arising from establishing a new regulatory framework specific to OTT services.

CCIA notes the Government of India’s ambitious agenda to modernize the regulatory framework for digital and telecommunications services in India. Internet companies operating in the global marketplace share many of the desired goals to support the next generation of digitally-enabled economic growth while strengthening trust and reliability in Internet services and communications. As the various initiatives take form, CCIA encourages policymakers in India to ensure a regulatory environment that will enable growth in digital services across the various sectors, avoid protectionist elements, and ultimately be to the benefit of all Internet users and entrepreneurs in India.

With respect to this consultation on regulating OTT services, CCIA offers three main considerations for TRAI. First, OTT services refer to a broad range of internet-enabled services that are subject to existing and likely forthcoming regulations, demonstrating that key regulatory goals can be addressed without introducing a new and confusing jurisdictional framework. Second, extending traditional telephony-style regulations to such services is unjustified and would likely instead bring widespread harms given the dynamic market response to the introduction of these new technologies.<sup>2</sup> Third, this consultation’s proposed steps to empower government entities and regulators to selectively block access to OTT services in India brings serious concerns with respect to internet freedom, privacy, and security.

---

<sup>1</sup> For more than 50 years, CCIA has promoted open markets, open systems, and open networks. For more, visit [ccianet.org](http://ccianet.org).

<sup>2</sup> CCIA has also provided relevant input in recent consultation with the Department of Telecommunications and TRAI regarding OTT regulations. See Comments on Telecom Bill 2022, <https://ccianet.org/library/comments-on-indian-draft-telecom-bill-2022/>; CCIA Comments on Regulatory Convergence <https://ccianet.org/library/ccia-comments-to-traai-consultation-on-regulatory-convergence/>.

## I. RESPONSES TO ISSUES RELATING TO REGULATORY MECHANISMS FOR OTT COMMUNICATION SERVICES

### Q1. What should be the definition of over-the-top (OTT) services?

**CCIA Response:** Generally, an OTT service is a type of service that is provided to the end-user over the public internet, or “over-the-top” of an existing network connection. Any definitions that TRAI adopts should encompass the evolving nature of OTT services and recognize that OTT and traditional telecom services as different from one another. Therefore, these two distinct services are not amenable to regulations that treat them as substitutable services from both a consumer and governance perspective.

#### **Justification:**

The term “OTT” encompasses a wide range of services delivered over the public internet. These services are dynamic and evolving in nature and include instant messaging, streaming, social networking, e-commerce, video conferencing, and many others. OTTs have been defined in a similar manner by the following; the OECD describes OTT services as being provided “over the Internet”<sup>3</sup>; the Office of Communications, United Kingdom uses the phrase “over the top of an existing data network connection”<sup>4</sup>; and the Body of European Regulators for Electronic Communications use the phrase “over the Public Internet”.<sup>5</sup>

When looking to define OTT services, it is important to emphasize the technical and business differences between TSPs and OTT services. It is therefore unhelpful for regulators to use notions of “substitutability” in defining OTT services, as suggested in the Public Consultation.<sup>6</sup>

From a technical perspective, OTT service providers operate at the application layer (i.e. the layer which rests above the layers responsible for complex network interactions and utilize the underlying network layer to transfer data or content). This is differential from with telecommunication service providers (TSPs) that operate at the network layer (i.e. the layer connecting different networks and driving the operation of the internet).<sup>7</sup> TSPs control the underlying broadband access infrastructure and are gatekeepers to broadband internet access, while OTT services require the TSP’s network to operate. TSPs are also granted exclusive rights to use and monetize spectrum, control critical network infrastructure, and to rights of way to build that infrastructure and provide interconnectivity services, and TSPs interconnect with the traditional PSTN/switched voice network. These functions all implicate

<sup>3</sup> Organisation for Economic Co-operation and Development (OECD) Communications Outlook (2013), at page 4, available at [https://www.potraz.gov.zw/wp-content/uploads/2016/01/Consultation\\_OTT.pdf](https://www.potraz.gov.zw/wp-content/uploads/2016/01/Consultation_OTT.pdf).

<sup>4</sup> The Office of Communications, United Kingdom, Mobile Call Termination Market Review 2015-18, at page 5, available at [https://www.ofcom.org.uk/\\_data/assets/pdf\\_file/0025/74257/annex\\_15\\_glossary.pdf](https://www.ofcom.org.uk/_data/assets/pdf_file/0025/74257/annex_15_glossary.pdf).

<sup>5</sup> Body of European Regulators for Electronic Communications, Report on OTT Services, 2016, at page 3, available at [https://www.berec.europa.eu/sites/default/files/files/document\\_register\\_store/2016/2/BoR\\_%2816%29\\_35\\_Report\\_on\\_OTT\\_services.pdf](https://www.berec.europa.eu/sites/default/files/files/document_register_store/2016/2/BoR_%2816%29_35_Report_on_OTT_services.pdf).

<sup>6</sup> The definition provided by ITU-T5 as cited in the Paper is that OTT is an application accessed and delivered over the public internet “that may be a direct technical/ functional substitute for traditional international telecommunication services”. The Paper also offers the following criteria to identify an OTT communication service: (i) it is accessed and delivered through an application over the public Internet, using the network infrastructure of TSPs; and (ii) “it is a direct technical/ functional substitute for traditional telecommunication services provided by TSPs”.

<sup>7</sup> TRAI has recognized the separation of layers with respect to internet telephony services. See Recommendations on Regulatory Framework for Internet Telephone (2017) (“The separation of network and service layers of telecom service offering is the natural progress of the technological changes in this domain. It is now possible to separate provision of service contents, configuration and modification of service attributes regardless of the network catering to such service.”).

specific regulatory rights and responsibilities. OTT services do not have any control or rights with respect to how telecommunication infrastructure is deployed in a region.

OTT services are also not perfect substitutes for TSPs. While TSPs offer only voice and SMS communication, OTT services offer a variety of dynamic services in addition to telephony and messaging services that are not offered by traditional TSPs such as video calling, audio recording, file sharing, group chats, payments, etc.<sup>8</sup> These services are unique to OTTs and form an inherent part of the overall service provided by them. OTT platforms also provide device synchronicity i.e., they can be accessed through multiple internet-enabled devices simultaneously whereas TSPs cannot because of the hardware requirement of a SIM card.<sup>9</sup> Given the rapid pace at which OTT platforms innovate and grow, these differences between OTTs and TSPs are likely to increase in the future.<sup>10</sup>

**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.**

**CCIA Response:** There is not a need to identify sub-categories of OTT services.

**Q3. What should be the definition of OTT communication services? Please provide a list of features which may comprehensively characterize OTT communication services.**

**CCIA Response:** It is not necessary to craft a definition for OTT communication services. CCIA reiterates that there are fundamental differences between OTT services and TSPs that make comparison inaccurate for classification purposes. Further, the imposition of rigid definitions based on specific distinguishing features that are likely to be soon obsolete would be actively harmful.

**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.**

**CCIA Response:** It is not necessary to create or focus on the sub-categories of OTT services, or even the sub categories of OTT communication services for purposes of regulation.

<sup>8</sup> BEUC response to the public consultation, The European Consumer Organisation, November 2015, available on <https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-ott-services>

<sup>9</sup> Esya Centre, Regulation of OTT communication services, January 2023, available on [https://static1.squarespace.com/static/5bcef7b429f2cc38df3862f5/t/63d8b49179bdf80b02924cc6/1675146395190/Esya\\_Centre\\_Report\\_Communications\\_OTT\\_Services.pdf](https://static1.squarespace.com/static/5bcef7b429f2cc38df3862f5/t/63d8b49179bdf80b02924cc6/1675146395190/Esya_Centre_Report_Communications_OTT_Services.pdf).

<sup>10</sup> The Economic and Societal Value of Rich Interaction Applications in India, November 2017, available on <https://broadbandindiaforum.com/wp-content/uploads/2020/12/THE-ECONOMIC-AND-SOCIETAL-VALUE-OF-RICH-INTERACTIONAPPLICATIONS-IN-INDIA.pdf>.

## **Justification (in response to Questions 2-4):**

It is neither helpful, nor practical, to classify or create definitions of subsets of different OTT services including OTT communication services.

There are various overlaps in the features and functions within OTT services, and the services offered are dynamic and constantly evolving. OTT services are often a blend of communication services with other services such as digital payments, discussion boards, notes, and screen sharing, with consumer troubleshooting, grievance, and redress mechanisms.

OTT services provide both communications based and non-communication-based features such as a ride hailing or food delivery, that also enables users to communicate with drivers and restaurants. For example, food delivery services such as Zomato and Swiggy facilitate messaging,<sup>11</sup> PayTM combines digital payments with messaging functionality (wherein one can message the person any payment is being made to or request any payment),<sup>12</sup> gaming applications such as Call of Duty: Mobile allow in-game messaging between players,<sup>13</sup> and rental applications like Airbnb encourages users to use the in-app messaging and communications feature to chat with the host.<sup>14</sup> Since it is typically one integrated platform or application providing these different services, creating a unique regulatory category for specific embedded services would lead to regulatory fragmentation and impose unfeasible obligations on these services.

Further, any test to make a distinction between communication and non-communication OTT services would require a case-by-case assessment. Such classification would lead to OTT applications that provide the same basic functionality being treated differently under the law, simply on account of the differences in degree of ancillary functionalities they offer.

Given that there can be a commonality of features that may exist between various OTT services, identifying different categories of OTT services is not feasible and should not be a focus of work for regulators.

### **Q5. 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**

<sup>11</sup> Zomato introduces a chat feature for online food ordering, Tech Desk, Indian Express, December 2015, available on <https://indianexpress.com/article/technology/social/zomato-introduces-a-chat-feature-for-online-food-ordering/>, Chatbot at Swiggy, Abey “AB” Alex, July 2019, available on <https://bytes.swiggy.com/chatbots-at-swiggy-6299116f9e69>

<sup>12</sup> Paytm takes on WhatsApp, launched inbox, in-app messaging feature, Kul Bhushan, November 2017; available on <https://tech.hindustantimes.com/tech/news/paytm-takes-on-whatsapp-launches-inbox-in-app-messaging-feature-storyiszDnbOAKPjHIPOdBgdWgJ.html>,

<sup>13</sup> Call of Duty: Warzone mobile limited release FAQ, Call of Duty, November 2022, available on <https://www.callofduty.com/blog/2022/11/Call-of-Duty-Warzone-Mobile-Limited-Release-FAQ>.

<sup>14</sup> Airbnb Help Centre, available on <https://www.airbnb.co.in/help/article/209/>.

- (e) Safety aspects;**
- (f) Quality of service aspects;**
- (g) Consumer grievance redressal aspects; and**
- (h) Any other aspects (please specify).**

**CCIA Response in General to Q5:** OTT platforms are sufficiently regulated under a robust framework and there is no need to create an additional specialized regulatory framework. Aspects such as security, privacy and safety, quality of service, and consumer redress are already regulated. Economic aspects should be left to market forces absent evidence of systemic market failure.

### **(a) Regulatory aspects**

**CCIA Response:** OTT services and licensed telecommunications services in India are operationally, technically, and functionally different. OTT services include any communications-related services operated by OTT services. Regulatory frameworks that focus solely on the final service offered, without taking into account the underlying technology, may lead to poorly thought-out regulations that fail to achieve the policy intent. Telecommunication service providers (TSPs) make use of valuable spectrum and manage network infrastructure, both of which are critical public resources necessitating government licensing and supervision. In contrast, over-the-top (OTT) services do not control or oversee the telecommunications infrastructure covered by licensing requirements. Rather, they exclusively deliver applications that the general public accesses through the public internet, which is operated entirely by TSPs/ISPs. Therefore, the imposition of a regulatory framework intended for TSPs should not be applied to OTT platforms.

That is not to say that OTT are not/should not be regulated. OTT services are already regulated by existing laws, including the Information Technology Act 2000 (IT Act) and allied rules. These include security provisions: lawful interception and encryption (Section 69, IT Act); takedown/blocking obligations (Section 69A, IT Act ); Privacy and safety obligations: privacy policies, obligations to collect, store and disclosure of sensitive personal data, (Information Technology—Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; penalty for breach of confidentiality and privacy (Section 72A, IT Act); power of the government to prescribe suitable methods of encryption (Section 84, IT Act); due diligence obligations under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Consumer grievance redress and quality of services for paid services under the Consumer Protection Act, 2019; and Corporate compliance under the Companies Act, 2013, among others. MeitY has been the appropriate regulatory body given its specialization in policy matters relating to IT, electronics and the internet, and administration of the IT Act. Extending regulatory oversight of these services to entities such as the Department of Telecommunications is not necessary and would lead to duplicative efforts that undermine consumer access to their preferred services, industry presence in the market, and the governing of digital services.

Moreover, OTT service providers are likely to be regulated under the recently passed Digital Personal Data Protection Act, 2023 (“DPDP Act”).<sup>15</sup> Further, based on public statements made by the Central Government, OTT services are likely to be regulated under the Digital India Act (“DIA”).<sup>16</sup> The need to harmonize the overlap in rules and regulations across various sectors has also been acknowledged by the Government in the public consultations held on the proposed DIA. The presence of fragmented laws on the same subject matter (i.e., regulation of online products or services) will increase the cost of compliance, impede effective attainment of legitimate regulatory objectives, and will lead to business uncertainty.

The imposition of similar regulatory frameworks, ignoring the underlying differences between OTT services and TSPs, is likely to cause regulatory imbalances and onerous compliance burdens that will have a serious impact on innovation and growth of the OTT sector.

It is also important for regulations to take into account the geographical scope of OTT services. Telecommunications services are typically offered on a country-by-country basis, reflecting the design of specific networks bound by a country’s jurisdiction. On the other hand, OTT services operate globally, with services and their associated benefits crossing national borders. In the event onerous obligations are imposed with the objective being to create a “level playing field” between TSPs and OTT services providing communication features, OTT suppliers may disable communication services in such markets and focus on services that may be classified as non-communication services. The reduction in OTT services offered in a market will limit customer choice in India, may slowdown research and development in new OTT communications technologies, and impact user experiences.

## (b) Economic aspects

**CCIA Response:** The OTT market is characterized by low barriers to market entry, healthy competition among numerous players, and multiple services options for users. This sector has contributed immensely to India’s growth. As the Consultation Paper details, OTT services have positively contributed to developed and developing economies. Reports estimate that a 10 percent increase in use of OTT apps corresponds with an average increase of USD 1 billion in additional global GDP daily.<sup>17</sup> The Consultation Paper also notes that the improvements in the efficiency of delivering data has lowered price of bandwidth/data, benefiting consumers. According to a study, an increase in OTT services had also increased consumer surplus to USD 98 billion (Rs 7 lakh crore) in 2017 in India.<sup>18</sup>

India is also one of the largest telecom markets in the world with a subscriber base of over 1.17 billion. It has been reported by the Indian Council for Research on International Economic Relations-Prosus Center for Internet and Digital Economy report on ‘State of India’s Digital

<sup>15</sup> <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>

<sup>16</sup> ‘Presentation made during the Digital India Dialogues on the proposed Digital India Act on 9th March in Bengaluru, Karnataka’, available at [https://www.meity.gov.in/writereaddata/files/DIA\\_Presentation%2009.03.2023%20Final.pdf](https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf) and ‘MoS Rajeev Chandrasekhar holds Digital India Dialogues in Mumbai on the Principles of the Digital India Act’, available at <https://www.pib.gov.in/PressReleaseDetailm.aspx?PRID=1926711>

<sup>17</sup> WIK, The Economic And Societal Value Of Rich Interaction Applications In India, November 2017, available on [https://www.wik.org/fileadmin/files/\\_migrated/news\\_files/WIK-BIF\\_Report\\_-\\_The\\_Economic\\_and\\_Societal\\_Impact\\_of\\_RIAs\\_in\\_India.pdf](https://www.wik.org/fileadmin/files/_migrated/news_files/WIK-BIF_Report_-_The_Economic_and_Societal_Impact_of_RIAs_in_India.pdf)

<sup>18</sup> Telecom OTT apps create \$98 billion consumer surplus: report, Komal Gupta, November 2017, available on <https://www.livemint.com/Technology/U1113Z44VaTCXNUPsbsvGP/Telecom-OTT-apps-create-98-billion-consumer-surplus-report.html>



Economy' that internet subscriptions have more than tripled from 248 million in 2014 to 820 million in September 2022, and could reach 1 billion by 2025.<sup>19</sup>

In addition, the Broadband India Forum's report on the Economic Value of the App Economy in India (2023) supports the theory of contribution of OTT services to revenues earned by TSPs. The report states:

[b]esides the direct effect of the app economy on the GDP, there are spill-over effects in the supply industries (computer hardware, telecommunication and ICT services). An increase in sales in the App Economy not only gives rise to an increase in GDP but also creates a multiplier effect through indirect and induced effects. This is because the value through digitalization is not limited only to the sector in which this happens but influences both downstream and upstream sectors in the entire supply chain.<sup>20</sup>

Any suggestion that OTT services “free ride” over telecom services and underlying network infrastructure are inaccurate, and calls for mandatory compensation mechanisms should be rejected. The economic relationship between OTT services and TSPs is symbiotic. OTT apps boost demand for data and network capacity and subscription services, leading to increased revenue for the TSP.<sup>21</sup> Consumers want access to the new and innovative OTT applications, and in turn, pay TSPs for an efficient and fast user experience. TSPs' own reporting confirms increased revenue from growth in subscriber base.<sup>22</sup>

This is supported by findings made by BEREC in October 2022 that found no evidence to justify implementation of a direct compensation mechanism, which resembles the ‘Sending Party Network Pays’ (“SPNP”) principle, and such a mechanism could present various risks for the internet ecosystem. Instead, BEREC notes that these two sets of entities are mutually dependent on each other. Notably, the demand from ISPs' customers for content drives demand for broadband access (and as a corollary, the availability of broadband access drives demand for content). Additionally, BEREC notes that there is no evidence of free riding.<sup>23</sup> BEREC has also confirmed this view in its response to the European Commission's Exploratory Consultation on ‘The Future of the Electronic Communications Sector and Its Infrastructure’ which closed on May 17, 2023, where BEREC notes that “Currently, actors contribute in different ways to the internet ecosystem: some for example provide access networks, others digital infrastructures or IP transit services, others content, applications and services, and others again provide digital skills, or a combination thereof.”

---

<sup>19</sup> Indian Council for Research on International Economic Relations-Prosus, State of India's Digital Economy, available at [https://icrier.org/pdf/State\\_of\\_India\\_Digital\\_Economy\\_Report\\_2023.pdf](https://icrier.org/pdf/State_of_India_Digital_Economy_Report_2023.pdf) (page 28)

<sup>20</sup> Broadband India Forum, Report on Economic Value of the App Economy in India, June 2023, at page 9, available at <https://broadbandindiaforum.in/wp-content/uploads/2023/06/Research-paper-on-THE-ECONOMIC-VALUE-OF-THE-APP-ECONOMY-IN-INDIA.pdf>.

<sup>21</sup> <https://www.esyacentre.org/documents/2023/1/31/regulation-of-ott-communications-services-justified-concern-or-exaggerated-fear>

<sup>22</sup> Bharti Airtel reported an increase of over 27% in revenue from mobile services for the first quarter of the financial year 2022-23. Reliance Industries Limited, in the Consolidated Results for Quarter Ended 31st December 2022, reported that Jio earned a record quarterly revenue of INR 29,195 Crore, up 20.8% from last year, driven by steady increase in both subscriber base and ARPU for the connectivity business, as well as higher realizations from digital services. See Consolidated results for quarter ended 31st December 2022, January 2023, available on <https://www.ril.com/getattachment/9f6b979c70bd-4517-b257-370e9449cf40/Financial%20performance%20for%20the%20quarter/nine%20months%20ended%2031%20Dec,%202022.aspx>

<sup>23</sup> BEREC, Preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs, October 7, 2022, available at [https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%202822%29%20137%20BEREC\\_preliminary-assessment-payments-CAPs-to-ISPs\\_0.pdf](https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%202822%29%20137%20BEREC_preliminary-assessment-payments-CAPs-to-ISPs_0.pdf).

Increasing the regulatory burden on OTT services is also likely to be detrimental to users in India. An additional regulatory framework will increase the cost of compliance for OTT platforms, which may be passed on to consumers in terms of higher prices. This will severely affect users' ability to access content and communicate over the internet using low cost/free services. Imposing a license will also increase barriers to entry, reduce competition and stifle innovation by raising the cost-of-service, start-up OTT players will be deterred from entering the market. This will present a threat to India's start-up ecosystem.

### **(c) Security aspects**

**CCIA Response:** There are several provisions under the IT Act that deal with the security and safety procedures that OTT services must adhere to in order to keep users safe online. No further regulation is required on the ground of 'security' as OTT services are already subject to appropriate regulation under the IT Act.

The Indian Computer Emergency Response Team ("CERT-In") is the national nodal agency that oversees cybersecurity in India. Compliances on cybersecurity are prescribed under the CERT-In Rules and are broadly applicable to a wide range of entities, including OTT service providers as well. The CERT-In Rules, among other things, require entities to report specific categories of cybersecurity incidents and designate a point of contact to communicate with CERT-In. CCIA notes that the CERT-In is also empowered under the IT Act to call for information and give directions to service providers, intermediaries, body corporates, etc.

Additionally, Section 43A of the IT Act states that corporations' handling of sensitive personal data or information ("SPDI") will be liable to pay compensation to affected persons if it is negligent in implementing reasonable security practices and procedures and causes wrongful loss or wrongful gain to any person. Such reasonable security practices and procedures have been provided under the SPDI Rules, along with other compliances pertaining to personal information ("PI") and SPDI. Insofar as OTT service providers handle PI or SPDI while providing OTT services in India, they would have to comply with the obligations outlined therein. More importantly, once the DPDP Bill is enacted, OTT service providers will continue to have incremental and possibly more onerous obligations to implement reasonable security safeguards to prevent data breaches.

In addition, the IT Act also has provisions that enable the State to undertake measures in the interests of national security, public order, etc. For example, the law empowers Government agencies to issue directions under Section 69 for interception, monitoring, decryption directions, and under Section 69A for blocking orders vis-à-vis unlawful content generated, transmitted, received, or stored in any computer resource. Such directions can be issued to intermediaries and / or persons in charge of a computer resource (such as OTT service providers) on specific grounds (such as sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States, public order, etc.). In addition, directions to monitor and collect traffic data or information for cyber-security purposes can also be issued under Section 69B.

Therefore, Section 43A, as well as Sections 69, 69A, and 69B are already applicable to OTT service providers under the framework of the IT Act, for not only ensuring security of PI or SPDI, but also assisting from a cybersecurity perspective.



#### (d) Privacy aspects

**CCIA Response:** As noted above, the SPDI Rules regulate body corporates (including OTT service providers) in their collection and processing of PI and SPDI. In this regard, OTT service providers have specific privacy-related compliances under the SPDI Rules. These include, among other things, the requirement to provide a clear and easily accessible privacy policy for the PI or SPDI being processed, to obtain informed consent for the collection and use of SPDI, to designate a grievance officer who must redress user grievances within specific timelines, and to adhere to the data minimization and retention requirements.

With the enactment of the DPDP, obligations on OTT service providers vis-à-vis maintaining the privacy of PI collected from their users will become heightened.

#### (e) Safety aspects

**CCIA Response:** In addition to adhering to the cybersecurity and data privacy obligations under the CERT-In framework and SPDI Rules referred to above, it should be noted that OTT services are themselves also focused on ensuring user safety. This is to provide a safe and secure experience to users of their services and ensure that no harm accrues to them while using such services. As part of this, several OTT platforms have safety features, such as two-step verification, the option to block or report other user accounts, and the ability for users to implement privacy controls (such as limiting the visibility of their profile pictures).

Several OTT services are already working to introduce additional security features and in-app solutions and to configure their application interfaces so as to reduce the circulation of spam and fake news and reduce online harassment. For instance, some entities flag to the user that a message on a platform has been forwarded multiple times or limit the number of times content can be forwarded). The forthcoming DIA is also expected to prescribe additional rules with respect to online safety.

#### (f) Quality of service aspects

**CCIA Response:** OTT services are greatly incentivized to maintain a high quality of service given the level of competition in the OTT sector and ease to switch from one OTT services to another.

It is inappropriate to subject OTT services to specific quality of service benchmarks in a similar manner to that of how the Department of Telecommunications regulates Quality of Service (QoS) requirements for TSPs. As TSPs own and operate the network and utilize spectrum, the obligation to ensure the quality of these services lies with the TSPs. Internet access is facilitated by TSPs, who offer the necessary last-mile connectivity to users, whether through broadband, wireless, or fixed-line connections. This last mile infrastructure is what enables consumers to access OTT and platforms in the first place. TSPs invest in building and upgrading their networks to provide reliable and high-quality internet access to consumers. The performance and reliability of the network, including factors such as bandwidth, latency, and packet loss, directly impact the QoS experienced by users accessing OTTs and platforms.

This has been reiterated in the CCI study which suggests that QoS offered by TSPs very strongly influences consumer choice.<sup>24</sup> This suggests that QoS is an important obligation for TSPs to comply with. Any obligation placed on OTTs to ensure QoS would be ineffective and impractical, as they do not have the capability to manage essential infrastructure, including the last mile access to users, and they would therefore be deemed liable for an outcome over which they have no control. Their role is primarily focused on delivering content and services over the internet, relying on the infrastructure provided by TSPs.

### **(g) Consumer grievance redress**

**CCIA Response:** Certain OTT services are already subject to grievance redress requirements under existing frameworks. For paid OTT services, the Consumer Protection Act 2019 allows consumers to file complaints in relation to any deficiency in services. Consumers can also report grievances while using social media platforms under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021).

**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?**

**CCIA Response:** There is not a need to bring OTT communications services under a new licensing/regulatory framework, and doing so would likely not benefit consumers or promote innovation.

### **Justification:**

As detailed throughout these comments, OTTs are already subject to broad regulatory oversight that ensures a competitive landscape, benefits consumers, and ensures further innovation in India's digital economy.

Regulatory intervention will increase compliance costs and create new barriers to entry. As noted in the CCI study "a separate regulatory framework for OTTs will only stifle technological innovation".<sup>25</sup> Given that OTT services operate in a market with low barriers to entry, only constant innovation can help OTT service providers distinguish themselves from other competitors and generate value with respect to their services. In addition to this, imposing onerous regulatory compliances (typically intended for traditional telecom services) on OTT services may not only adversely affect the ease of doing business in India, but also compel OTT service providers to scale back investments in technology innovation and pass on financial burdens to users. This may occur in scenarios where users end up being charged for using OTT services. This will adversely impact users who cannot afford paying for such services – and thus increase the digital divide in India. A licensing regime (especially one that spans several

<sup>24</sup> Market Study on the Telecom Sector in India, Competition Commission of India, December 2021, available on Pg 16, <https://www.cci.gov.in/images/marketstudie/en/market-study-on-the-telecom-sector-in-india1652267616.pdf>

<sup>25</sup> Market Study on the Telecom Sector in India, Competition Commission of India, December 2022, available on <https://www.cci.gov.in/images/marketstudie/en/market-study-on-the-telecom-sector-in-india1652267616.pdf>

years and contains heightened compliances) may impinge on the ability of OTT services to evolve over time and adapt in the face of newer technologies.

**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:**

- 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.)

**CCIA Response in General to Q7:** No additional licensing/regulatory framework is required for OTT services as a whole, as they are already subject, where appropriate, to relevant regulations.

#### **(a) Lawful interception**

**CCIA Response:** Section 69, Section 69A and Section 69B deal with different powers of the State to: (a) intercept, monitor and decrypt information generated, transmitted, received or stored in a computer resource (Section 69); (b) block public access to information generated, transmitted, received, stored or hosted in any computer resource (Section 69A); and (c) monitor and collect traffic data or information generated, transmitted, received or stored in a computer resource (Section 69B). Please refer to the response to question 5 on ‘security aspects’ for further details.

#### **(b) Privacy and security**

**CCIA Response:** The CERT-In framework, along with the SPDI Rules contain a host of obligations to tackle cyber-security incidents and maintain the privacy of PI or SPDI of individuals. Please refer to the response to question 5 above on ‘privacy aspects’ and ‘security aspects’ for further information.

#### **(c) Emergency services**

**CCIA Response:** The CP refers to public utility or emergency services that TSPs are required to provide under the Unified License framework. These include emergency services such as toll-free services for police, fire, and ambulance. The idea behind requiring TSPs to, for example, enable toll free services is to ensure that subscribers are not charged for making calls during an

emergency, or are not placed at a disadvantage for not being able to make such calls (such as on account of low account balance for pre-paid numbers).

With regard to whether OTT service providers should be mandated to offer emergency services, CCIA's position is that they should not be subject to any requirements in this regard. This is because:

- OTT services need the internet to operate and function, and thus may not be best placed to provide emergency services to their users (especially since the internet may not always be available to a user);
- Most OTT service providers do not connect to the PSTN or have the infrastructure or technical capability in place to provide emergency calling services (or even convey emergency announcements);
- To provide emergency services in relation to search and rescue operations, it is critical that an individual's geo-location be ascertained. However, OTT service providers do not necessarily have access to the same (such as on account of privacy settings on a platform). They may, in turn, be compelled to rely on third-party tracking services in order to provide such emergency services; and
- The infrastructure of first responders, like fire and police stations, is predominantly optimized for managing communications via conventional telecommunication services linked to the PSTN network. These facilities might lack the essential incorporation of OTT services, which presents a difficulty in efficiently handling emergency calls that originate from OTT platforms. This lack of seamless compatibility results in a notable void within the emergency response framework, as individuals who exclusively depend on OTT services could find themselves without a direct means of communication with emergency services.

#### **(d) Unsolicited commercial communications (“UCC”)**

**CCIA Response:** As user trust and convenience are key factors for OTT services, there is constant investment and improvement in services with an aim to reduce UCC. OTT services that enable commercial communication on their platforms have proactively implemented features that allow users to report or block the senders of unsolicited commercial messages and calls.

These services deploy extensive safety measures such as automated filters to detect fake/spam emails. Users have an option to block messages from certain users, report user profiles. For example, WhatsApp uses the ‘silence unknown callers’ feature to filter out spam calls and Meta applies spam detection on spot AI technology to take down accounts that show abnormal behavior. Instagram also uses tools to report undesirable and spam content and allows users to report and block accounts and messages through their settings. Platforms like Snapchat use Google’s safe browsing which notifies webmasters when their websites are compromised by malicious actors and helps them diagnose and resolve the problem so that their visitors stay safer.

### (e) Customer verification

**CCIA Response:** OTT services typically undertake verification of any user who signs up for their services, either by way of phone number or email verification (such as via OTPs). It may also be noted that the IG Rules also mandate certain intermediaries to enable users to voluntarily verify their accounts by using any appropriate mechanism (including an active Indian mobile number). To this extent, OTT providers (that qualify as significant social media intermediaries) are already subject to such verification requirements.

In addition, CCIA notes that certain OTT service providers have entered into voluntary arrangements with regulatory authorities to tackle instances where users with disconnected phone numbers continue to use an OTT service where they have signed up using such numbers, by undertaking a re-verification of such numbers.

It would also be helpful for additional clarity with respect to whether the intent of customer verification obligations is with respect to law enforcement or for identification of users/senders during messages. At the point of accessing the internet, Know Your Customer (“KYC”) verification processes already exist that enable detection of users. Creating additional KYC obligations on OTT services that operate on the internet is likely to create redundancies. This will affect the ease of accessing the internet. At present, there are adequate KYC related obligations in place applicable to both TSPs and OTTs, depending on the level of risk they pose.

### (f) Quality of service

**CCIA Response:** Please refer to the response to question 5 above on ‘quality of service aspects’.

### (g) Consumer grievance redress

**CCIA Response:** Please refer to the response to question 5 above on ‘consumer grievance redress aspects’.

### (h) Eligibility conditions

**CCIA Response:** This is not applicable, since CCIA believes that there is no need to introduce any new licensing or regulatory framework for OTT service providers.

As has been mentioned earlier, OTTs do not use public resources such as spectrum or rights of way to operate. They operate on the internet and therefore conditions similar to the Unified License (UL) are misconceived and inappropriate to be extended to OTTs. The internet is an open and globally competitive domain. Imposing eligibility conditions on OTTs similar to the technical, operational, and financial conditions imposed on TSPs under the UL will increase costs of operation which will ultimately result in higher costs for customers. The increase in cost of service will act as an entry barrier, particularly for start-ups, ultimately stifling both innovation and competition. This will also have a detrimental impact on India’s digital economy.

## (i) Financial conditions

**CCIA Response:** This is not applicable, since there is no need to introduce any new licensing or regulatory framework for OTT service providers.

**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?**

**CCIA Response:** While collaboration is an important element to the existing environment among all stakeholders, there is not a need for a formal regulatory framework between OTT communication services providers and the licensed telecommunication service providers. Mandating collaboration could empower TSP's to seek anticompetitive benefits as a condition for accessing their networks, undermining consumer benefits. Presently, OTTs and TSPs collaborate in mutually beneficial arrangements that are driven by market forces. Imposing a formal regulatory framework will skew the market balance as it will entrench the role of TSPs as gatekeepers to the internet, ultimately impacting the open nature of the internet and services provided on it.

### **Justification:**

CCIA emphasizes that collaboration among all stakeholders in the digital environment with respect to access and investment to networks is critical. Many of the elements for a collaborative framework between TSPs and OTT services detailed in the Consultation Paper already exist, demonstrating the symbiotic and mutually beneficial relationship among these actors. OTT service providers make significant investments in the development of complementary internet infrastructure across the globe.

This includes:

- **Caching and use of Content delivery networks (“CDNs”).** Caches refers to the practice of storing a copy of data that enables future requests for that data to be delivered faster than if the request was sent to access the data’s primary storage location.<sup>26</sup> CDNs deploy networks of caching servers to bring content closer to the end user.<sup>27</sup>
- **Partnerships on submarine cables.** OTT and telecommunications providers also have partnerships to build submarine cables as well as to manage internet traffic, including significant recent investments from OTT providers to improve connectivity.<sup>28</sup> These

<sup>26</sup> <https://www.internetsociety.org/blog/2022/09/sender-pays-what-lessons-european-policy-makers-should-take-from-south-korea/>.

<sup>27</sup> See Expanding Cloudflare to 25+ Cities in Brazil, <https://blog.cloudflare.com/expanding-to-25-plus-cities-in-brazil/>; <https://cloud.google.com/blog/products/networking/introducing-media-cdn>.

<sup>28</sup> Meta has partnered with Airtel to develop subsea cable infrastructure, and Google has also been involved in subsea cable projects to improve global connectivity, including in India, available at <https://indianexpress.com/article/business/airtel-partners-with-meta-to-develop-undersea-cable-infra-for-high-speed-internet-8307705/> and <https://cloud.google.com/blog/products/infrastructure/announcing-the-blue-and-raman-subsea-cable-systems>.



partnerships will continue to increase, also considering trends already visible in the telecommunications industry, such as the virtualization of networks. Networks are shifting from a hardware to a software base, such as through the cloud, with an evident necessity for collaboration between the two industries and the need to support the uptake of cloud services.

- **Tailoring services based on network capacity and device type.** The vast majority of OTT providers—particularly the largest operators—deliver their audiovisual content to the consumer based on the bandwidth available. Streaming providers do not send the same volume of traffic for the same content to each user that demands it—for consumers attempting to access the content with a slower broadband connection, OTT providers generally lower the burden on the broadband network to ensure that the content *does* reach the end-user. Similarly, for consumers accessing content on a mobile device, resolution, and thus bandwidth requirements, differ from that of fixed networks and suppliers adjust the stream accordingly. Investments in efficient delivery of services by OTT providers based not only on network placement or infrastructure but the actual traffic being sent play a key role in the internet ecosystem and relieving the strain on telecom providers’ networks.

In India, several OTT service providers have invested in these passive infrastructure and connectivity projects to provide better internet access services.<sup>29</sup> There have been several collaborative initiatives between TSPs, development agencies and OTT service providers aimed at investment in network infrastructure.

A report by Analysys Mason on ‘The Impact of Tech Companies’ Network Investment on The Economics of Broadband ISPs’ examines the demands posted by ISPs seeking compensation (by way of a network usage fees) from OTT service providers for carriage of traffic.<sup>30</sup> In this context, the report notes that in order to deliver their content and applications to end-users more efficiently, OTT service providers invest significant amounts in hosting, transport, and delivery networks. OTT service providers have continued to increase their investment, and it is estimated that on average, between 2018 and 2021, the investment was approximately \$120 billion annually. These investments complemented investments made by other stakeholders, like ISPs, to enable the functioning of the internet. In addition, according to Analysys Mason, collaboration between OTT service providers and ISPs has been key to the growth of the internet and the same is fundamentally driven by the corresponding rise in demand for online services and for broadband. Moreover, as OTT service providers continue to invest significant amounts in internet infrastructure, this improves service delivery to end users (by bringing content closer to them), and also provides cost savings to ISPs (approx. USD 5 to 6.4 billion each year, globally).<sup>31</sup>

In light of the above, and given the fact that free market practices already promote collaboration between OTT service providers and TSPs take place and enable them to benefit from one another, imposing any additional regulations on OTT services with respect to a more collaborative framework should be avoided.

<sup>29</sup> *Id.* Also as per reports, an industry alliance was founded by Meta to create network architectures to improve telecommunication infrastructure, available at <https://telecominfraproject.com/facebook-partnering-to-build-the-telecom-infra-project/>.

<sup>30</sup> Analysys Mason, The Impact of Tech Companies’ Network Investment on the Economics of Broadband ISPs, October 2022, at page 16, available at <https://www.analysismason.com/contentassets/b891ca583e084468baa0b829ced38799/main-report---infra-investment-2022.pdf>.

<sup>31</sup> *Id.* at p. 58.

**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?**

**CCIA Response:** Regulatory intervention in establishing a formal regulatory framework between OTT services and TSPs raises numerous concerns and would harm the internet ecosystem in India.

**Justification:**

First, a mandatory payment requirement is likely to lead to reduced investment in network architecture, a decrease in innovation, increased prices and worse online experiences for end users,<sup>32</sup> and would not ensure stable, long-term financing for infrastructure.

A formal regulatory framework could essentially result in double charging for the same infrastructure. In general, the creation of the fees would ultimately harm consumers: network fees may require OTT providers to reduce investment in their services and/or raise prices; also, network fees would create incentives to telecom companies to reduce network investment and not focus on innovation. Finally, there is no guarantee that mandatory fees will be invested to the benefit of consumers.

It is helpful to look at other countries' approaches to regulating the business partnerships among OTT providers and telecommunication providers. In 2016, South Korea introduced a mechanism to regulate traffic among market participants.<sup>33</sup> Studies show that this regime has the opposite effect to the intended objectives. In Korea, it has reduced investment (evidenced by fewer CDNs, not more; little use of Internet Exchange Points; reluctance to land new cables), led to lower quality of service (the result of fewer CDNs) and has increased the prices for the end user.<sup>34</sup>

Further, as a direct result of being pressured to pay high network fees to telecom providers, numerous South Korean and foreign content providers degraded their services,<sup>35</sup> moved abroad, or simply exited the market.<sup>36</sup> This led to higher latency rates, with South Korean internet users now having the worst latency experience of all OECD countries.<sup>37</sup> For the same reason, smaller Korean OTT providers and startups increasingly encounter difficulties entering the market or expanding their market share. This has greatly reduced competition for internet

<sup>32</sup> <https://blog.cloudflare.com/eu-network-usage-fees/> ("The Internet works best – fastest and most reliably – when networks connect freely and frequently, bringing content and service as close to consumers as possible. Network usage fees artificially disincentivize efforts to bring content close to users, making the Internet experience worse for consumers."); <https://itif.org/publications/2022/11/07/consumers-are-the-ones-who-end-up-paying-for-sending-party-pays-mandates/>.

<sup>33</sup> [https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf?\\_\\_blob=publicationFile&v=1](https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf?__blob=publicationFile&v=1).

<sup>34</sup> <https://researchictolutions.com/home/wp-content/uploads/2022/11/RIS-Europe-FINAL.pdf>

<sup>35</sup> [https://carnegieendowment.org/files/202108-KoreanWayWithData\\_final5.pdf](https://carnegieendowment.org/files/202108-KoreanWayWithData_final5.pdf).

<sup>36</sup> [https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf?\\_\\_blob=publicationFile&v=1](https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf?__blob=publicationFile&v=1).

<sup>37</sup> <https://www.oecd-ilibrary.org/docserver/755e2d0c-en.pdf?expires=1662914824&id=id&accname=guest&checksum=6120E5C2732B20A83010C828A73EA916>.

access services in South Korea and led to sharp decreases in the level of services and content available to consumers. Surprisingly perhaps, the roll-out of 5G networks in South Korea is also slowing down, even though the country is often perceived as a mobile tech champion by many abroad.<sup>38</sup>

Second, a new remuneration requirement undermines net neutrality principles. Network usage payments are inherently about arbitrary mechanisms for treating certain data traffic differently and strengthening their control over users' access to the internet. The introduction of network fees will lead to the creation of a two-tiered internet. Companies who can pay telecommunications providers to reach their customers may be treated preferentially, for example with better services, cementing their advantageous position. By contrast, OTT providers that cannot – or refuse to – pay, could be discriminated against, with lower quality service.

Further, CCIA understands that TSPs in India recently advocated for a revenue-sharing model with OTT players for the usage of their network infrastructure. However, industry stakeholders and think tanks have raised concerns with the same. These are largely in line with the concerns highlighted by us above.

- As per CUTS International, subjecting OTT service providers to *“additional unreasonable regulations” may negatively affect consumers...in particular, smaller OTT service providers that provide offer customised content to consumers may not be in a position to enter into mutually beneficial cost-sharing pacts with the telecom operators.*<sup>39</sup>
- Additionally, a revenue sharing model may also pose disadvantages to consumers. For example, consumers may face an increase in cost of services as they will not only have to pay TSPs for network access but also OTT service providers for their services (assuming that OTT service providers begin charging - or begin charging more - for their services in order to further compensate TSPs).
- Another concern is that a revenue sharing model may lead to a decrease in the quality of services of OTT platforms, as OTT service providers may be forced to redirect investment intended for, among other things, improving their services towards making payments to TSPs.
- The Internet and Mobile Association of India (“IAMAI”) has also opposed the concept of revenue sharing between OTT service providers and TSPs. As per the IAMAI, any framework that follows the SPNP model may allow TSPs to exploit internet businesses by formalizing ‘rent seeking’. This would adversely impact India’s digital economy and the creative ecosystem it sustains.
- The IAMAI has also stated that imposing any additional higher costs associated with internet usage may disincentivize growth of OTT services in India and reduce their overall revenues. A revenue sharing model may also strike at the principle of net neutrality.

<sup>38</sup> <https://www.reuters.com/business/media-telecom/skoreas-high-speed-5g-mobile-revolution-gives-way-evolution-2022-05-13/>.

<sup>39</sup> ‘OTT regulation should keep consumer interest in consideration: CUTS International’, available at <https://cuts-ccier.org/ott-regulation-should-keep-consumer-interest-in-consideration-cuts-international/>

## II. ISSUES RELATING TO THE SELECTIVE BANNING OF OTT SERVICES

At the outset, recognizing and acknowledging the internet's transformative power, CCIA asserts the fundamental importance of maintaining continuous internet access, allowing for only exceptional circumstances where a partial reduction of services might be warranted.

Before delving into the technical and regulatory aspects of selectively banning OTT services, it's essential to assess India's current internet shutdown framework. The Parliament's Standing Committee on Communications and Information Technology (SCIT) 26th Report highlights the absence of official shutdown records, expressing disappointment in the MHA and DoT for inadequate tracking. This data gap hinders the understanding of whether shutdowns comply with the safeguards outlined in the 2017 Telecom Suspension Rules and Supreme Court directives. Public databases reveal internet shutdowns are routinely enforced for administrative or routine policing activities, and not for major safety concerns.

CCIA therefore calls upon the Department of Telecommunications to establish a transparent database accessible to the public, dedicated to documenting all instances of internet shutdowns across the nation. The DoT should then conduct a comprehensive analysis of these shutdown directives, assessing their adherence to legal, constitutional, and judicial safeguards. The outcomes of this evaluation should be shared publicly, and a platform for thorough examination and dialogue among a diverse range of stakeholders, encompassing the academia, business and consumer representatives, and civil society. Such efforts would not only contribute to preventing the adverse effects of internet shutdowns in the country but also facilitate a comprehensive discourse on effective strategies to mitigate these consequences.

**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.**

**CCIA Response:** There are several technical and security challenges to selective banning of specific OTT services.<sup>40</sup>

- **URL-level blocking:** Websites often have fixed domain names, and consequently easily identifiable URLs and IP addresses. On account of this, it is possible to selectively ban websites – including websites operated by OTT service providers. However, users are still able to get around this. They may rely on another domain name (if available) for the same online product or service that has been selectively banned in order to access the same. They may also use VPN services (whether domestic or foreign) to bypass such a ban.
- **Application-level blocking:** The same can be done either by an OTT service provider itself, or by a TSP. For an OTT service provider to block services in a specific geographic area, it will need the location information of its users. Accessing such information poses privacy concerns, especially given the fact that India's upcoming data privacy law

<sup>40</sup> See Selective Banning of OTT applications, Parag Kar, July 2023, <https://paragkar.medium.com/selective-banning-of-ott-application06a740ab69d>

imposes heightened compliances vis-à-vis collection and processing of PI, such as an individual's geo-location. Moreover, OTT providers may have to seek permission from users to access their location information – and users may not always be willing to grant such permission.

- **TSP-level blocking:** Blocking can be done using the destination IP addresses of all the servers used by an OTT service provider. However, TSPs may still face challenges with this process as an OTT service provider may be reluctant to share its IP addresses, since sharing the same may expose it to potential cyber-security incidents. Additionally, and as already noted by the DoT, the destination IP addresses of servers used by OTT services providers are often hosted on the cloud and tend to be dynamic (for example, to prevent tracing by bad actors).
- Selective banning can lead to over-blocking. There may be various other OTT services hosted on the same cloud service and using the same (albeit dynamic) IP address, as an OTT service that the Government seeks to selectively block. Thus, the possibility that relying on any such IP address may cause unaware OTT services to be blocked cannot be ruled out.
- One possible method to avoid such a scenario is for TSPs to conduct deep-packet inspection. That is, if IP addresses are somehow accessed in real-time through URL mapping (i.e., by physically checking every URL), TSPs may have to investigate each packet of data being sent over the internet to examine the origin, destination as well the content of such data packet and correctly identify which specific OTT service they intend to block. This approach will, however, lead to far-reaching privacy and free speech concerns, since users' communications will have to be intercepted and examined at the TSP level to merely pursue the selective banning of an OTT service.

**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?**

**CCIA Response:** There is no need for an additional 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. The IT Act is already used to block online content in India. There are significant risks to Internet freedom and expression online, public safety, and security with increased blocking of Internet services.

**Justification:**

As noted above in this document, there are existing provisions that enable the blocking of content on recognized grounds. For example, Section 69A of the IT Act read with the Blocking Rules may be used to block online content (such as a specific URL or online post), or even an entire platform if required on grounds relating to the sovereignty and integrity of India, national security, public order, etc. As noted above, the Government has previously already relied on Section 69A to selectively block entire OTT platforms in the interests of national security, and to

ensure that they cannot be accessed within India. Similarly, under Section 79 of the IT Act read with the IG Rules, access to online content can be blocked under certain grounds.

Therefore, there is no requirement for a new policy on selective banning of OTT services and the aforementioned existing provisions under the IT Act can be relied on. This will ensure there is no undue interference with the public's right to access an OTT service, and an OTT service's ability to offer its platform to its users. Another advantage of the current legal framework is that it empowered regulatory authorities to primarily target bad actors that are active on online platforms.

Further, MeitY is the appropriate ministry for regulating OTT services and for deliberations on banning OTT services and websites. MeitY possesses the necessary expertise, knowledge, and authority to assess the implications and considerations related to internet services bans comprehensively. This should include taking into account both constitutional and international commitments to both economic and human rights, particularly the right to freedom of opinion and expression; including the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. TRAI and the DoT should defer this question of selective banning of these services to MeitY for consideration.

Finally, the risks associated with expanded internet shutdowns or blocking must be considered in this context. As the Consultation Paper notes, there are social, economic, and human costs associated with internet shutdowns. Internet shutdowns interfere with the rights to freedom of opinion and expression, access to information, and freedom of assembly, among many other rights.

Restricting access to internet services brings significant consequences, affecting many sectors including education, healthcare, communication, e-commerce, and many more.<sup>41</sup> Access to information, freedom of expression, and the ability to connect with others are severely hindered, leading to significant disruptions in daily activities and impeding economic growth. In 2016, a study by the Brookings Institution pointed out that shutdowns drained USD 2.4 billion from the global economy between 2015 and 2016. Shutdowns also destabilize the income for people who rely on the internet to run and promote their small businesses and enterprises. They particularly negatively affect women and other marginalized groups, who rely on the internet to make a living—cutting or disrupting access to the internet means denying them their capacity to afford basic necessities, such as food, water, electricity, and education for their families.

Access to online services through the internet is also a matter of health and public safety. As has been felt particularly acutely during the Covid-19 pandemic, without internet access, people are struggling to communicate with their families and loved ones. Most worryingly, the risks for minority groups are being compounded, as they are denied access to the health information provided by appropriate authorities such as the WHO and other experts that could save their lives. The COVID-19 pandemic has amplified the need for access to universal, resilient, open, secure, and affordable access to information and communications technologies

---

<sup>41</sup> Anatomy of an Internet Blackout, Indian Council for Research on International Economic Relations, April 2018, [https://icrier.org/pdf/Anatomy\\_of\\_an\\_Internet\\_Blackout.pdf](https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf)





for all. As reiterated by the United Nations Director-General, access to credible and timely information and communications tools are of paramount importance to stop the spread of the virus and advance public health. Preparation for future such emergencies requires protecting access to these services and refraining from policies that would jeopardize the country's ability to prevent another major pandemic in future which, without guaranteed access to internet resources, would destabilize the country's economy and the well-being of its people.

### **III. CONCLUSION**

CCIA appreciates the opportunity to provide its views in this consultation and supports TRAI for undertaking a detailed analysis of, and seeking stakeholder inputs on the potential consequences in establishing a new regulatory framework specific to OTT services.