

**From:** [amehra@usinfoundation.org](mailto:amehra@usinfoundation.org)

**To:** "Akhilesh Kumar Trivedi" <[advmn@traigov.in](mailto:advmn@traigov.in)>

**Sent:** Saturday, September 2, 2023 2:37:04 AM

**Subject:** USISPF Submission - TRAI CP on Regulatory Mechanism for OTT Communication Services, and Selective Banning of OTT Services

Dear Sir,

Greetings from the US-India Strategic Partnership Forum (**USISPF**).

Thank you for the opportunity to provide feedback on the TRAI Consultation Paper on **"Regulatory Mechanism for Overt-The-Top (OTT) Communication Services, and Selective Banning of OTT Services."**

Please see attached our submission for your consideration.

Thank you.

Kind regards,

Amiya

Amiya Mehra

Director, Digital Economy and TMT

US-India Strategic Partnership Forum (USISPF)

12 Hailey Road, New Delhi 110001

Ph: [+91 7042555990](tel:+917042555990)

E-mail: [amehra@usispf.org](mailto:amehra@usispf.org)

Website: [www.usispf.org](http://www.usispf.org)



**USISPF Comments on TRAI Consultation Paper on  
Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective  
Banning of OTT Services**

**A. Issues Related to 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.**

**USISPF Response:** As highlighted in this Consultation Paper, "...changes in network technology have supported the creation of an *ecosystem of online applications* including over-the-top (OTT) services...". OTT service providers operate on 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). The term "OTT" refers to a wide range of services that are provided over the internet, including online buying and selling, instant messaging, streaming, social networking, digital news, search services, navigation services, ride hailing services, delivery and logistics services. As clarified by the Body of European Regulators for Electronic Communications (BEREC) in a January 2016 report, "OTT" does not refer to a particular type of service, but to a method of provision.<sup>1</sup> We believe that one definition of "OTT" will not be able to encompass diverse functions and evolving technology.

- 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.**

**USISPF Response:** OTT services may have multiple functions that are inextricably interlinked. One application may require several features to work in tandem to provide a particular service. For example, a ride-hailing OTT application connects drivers to passengers, enables communication between drivers and passengers, plans routes, enable payments etc. Any attempt to delineate any of these features for the purpose of creating sub-categories of OTT services would be artificial and could lead to market fragmentation. Therefore, we believe it would be impractical and unnecessary to create classifications of OTT services.

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

AND

- 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.**

**USISPF Response:** Classifying OTT services based on whether they offer communication services is overly simplistic, impractical, and arbitrary. OTT services, similar to all digital services delivered over the internet, involve an element of interactivity and communication. An attempt to identify and define a separate sub-category of "OTT communication services" fails to recognise that OTTs blend communication services with other services. Moreover, services not categorised as "communications" today may include such features in the future. Given the evolving nature of technology and the dynamic nature of the services being provided over the internet, we do not recommend arriving at one definition of "OTT communication services."

---

<sup>1</sup> Body of European Regulators for Electronic Communications, Report on OTT Services, 2016, at page 3: [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)

In this Consultation Paper, TRAI defines OTT communication services as: (i) services accessed and delivered through an application over public internet, using the network infrastructure of telecom service providers (**TSPs**); and (ii) direct technical or functional substitutes for traditional telecom services provided by TSPs. We believe this definition is not entirely accurate.

As explained in our response to (1), the OTT ecosystem operates at the application layer above the telecommunications infrastructure and network layers of the interconnected telecommunications systems. However, OTT services are not substitutes of traditional telecom services. The key points of difference are as follows:

- At an operational level, OTT services cannot be used without relying on services provided by TSPs. Historically, internet applications, including OTT services, have driven data consumption and subsequently contributed to telecom network revenues. The International Telecommunication Union (**ITU**) released a study in 2020 entitled “Economic Impact of OTTs on national telecommunications/ICT markets.”<sup>2</sup> This study highlights the symbiotic relationship between OTT and telecommunications operators, stating “the exponential increase in data traffic and use of OTTs results both in new subscribers for broadband services and existing subscribers upgrading their subscriptions for greater speed and bandwidth.” As highlighted in this Consultation Paper, data released by TRAI also indicates that OTT services are driving data consumption, which accounted for 85.1% of TSP revenues as of December 2022. Accordingly, OTTs are complementary rather than substitutive of TSPs and depend on network services provided by TSPs.

The difference in infrastructure and delivery methods is another point of difference between OTT services and TSP services. The proposed definition of “OTT communication service” fails to recognize that certain services, including cloud-based communication services or services such as SaaS (software-as-a-service), B2B and enterprise communication services have specialized features that distinguish them from traditional telecom services. Such services are not operational or functional substitutes of traditional telecommunication services and do not always rely on the underlying telecom infrastructure to deliver their services. For instance, they may invest in their own infrastructure, including data centres, to effectuate delivery of their services.

- At a technical level, a key point of difference is that TSPs control and enjoy the rights to use and monetize critical resources on which the application layer is dependent. Telecommunications network operators have the right to acquire spectrum, obtain numbering resources, interconnect with the Public Switched Telephone Network (**PSTN**) and use the public right of way to set up telecom infrastructure. In contrast, OTT service providers depend on the manner in which TSPs choose to deploy their infrastructure and provide internet access.
- In terms of offerings, OTT service providers offer a broader range of services to users, which are not provided as part of traditional telecommunication services. For instance, features such as group chat, in-app content sharing (photos, stickers and GIFs), document sharing, geo-tagging of images, online payments interface, etc. are not part of traditional telecommunication services. Therefore, certain OTT services should not be considered “OTT communication services” or substitutable with services provided by TSPs simply because their features include voice and video calling and messaging.

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

- 1. regulatory aspects;**
- 2. economic aspects;**

---

<sup>2</sup> [https://www.itu.int/dms\\_pub/itu-d/oth/07/23/D07230000030001PDFE.pdf](https://www.itu.int/dms_pub/itu-d/oth/07/23/D07230000030001PDFE.pdf)

3. security aspects;
4. privacy aspects;
5. safety aspects;
6. quality of service aspects;
7. consumer grievance redressal aspects; and
8. any other aspects (please specify).

**USISPF Response:** OTT platforms are sufficiently regulated. Aspects such as security, privacy and safety, quality of service and consumer redressal are already regulated under existing laws. Economic aspects should be left to market forces. Please see our responses to (1) – (8) below.

**Regulatory Aspects:** Article 39(b) of the Indian Constitution provides that the State needs to direct its policy in such a manner that “the ownership and control of the material resources of the community as so distributed as best to subserve the common good.” In the context of telecommunications, telecommunications network operators have the right to acquire spectrum, obtain numbering resources and interconnect with the PSTN. They are also entitled to use the public right of way to set up telecom infrastructure. As highlighted in our response to (3) and (4), OTT services are not substitutes of traditional telecommunication services. It is on account of these rights of exclusivity over the distribution of public infrastructure that telecom operators have been traditionally subject to rigorous regulatory frameworks in India, including licensing regimes.

In contrast, OTT services that run on the application layer do not distribute natural resources or exercise control over the underlying spectrum. The services are offered over the internet and heavily depend on the data provided by TSPs. Accordingly, OTT services should not be regulated under the same regime as licensed telecommunication services. The imposition of similar regulatory frameworks, agnostic to these differences, is likely to cause regulatory imbalances and onerous compliances that will have a serious impact on innovation and growth of the OTT sector.

Moreover, OTTs are not exempt from regulations. OTT services are already regulated under existing regulatory frameworks, including the: Information Technology Act, 2000 (**IT Act**) and the rules thereunder. These include the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**SPDI Rules**), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (**Interception Rules**), the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (**Blocking Rules**), the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (**CERT-In Rules**), the CERT-In Directions of April 2022<sup>3</sup> (**CERT-In Directions**), and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**IT Rules, 2021**). The Consumer Protection Act, 2019, Competition Act, 2002, Companies Act, 2013 etc. also provide sufficient regulation and checks and balances to ensure that the OTT services industry is adequately regulated. Further, OTT service providers will also be regulated under the new Digital Personal Data Protection Act, 2023 (**DPDP Act**) and are likely to be regulated under the upcoming Digital India Act (**DIA**), which is set to replace the existing IT Act.

The open nature of the internet has been key to the growth of OTTs. Overregulation would stifle innovation and increase market entry barriers, hampering the growth of the sector.

**Economic Aspects:** TSPs and OTTs are interdependent and OTTs support the growth of TSPs. As observed by TRAI in this Consultation Paper, TSPs have gained a new source of revenue due to the widespread use of OTT services in the country. The rising demand for OTT services drives consumers to subscribe to higher-tier (and often more expensive) mobile data plans and internet services offered

---

<sup>3</sup> That is, the ‘Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet’, issued by the Indian Computer Emergency Response Team dated April 28, 2022.

by TSPs. The demand for OTT services not only creates a greater demand for internet access delivered by TSPs, it also enhances the overall quality and reliability of internet services, benefitting both OTTs and TSPs. OTT service providers also invest in complementary internet infrastructure to facilitate delivery and global functioning of their services.

There is growing evidence suggesting that TSPs benefit from the proliferation of OTTs. In the TRAI Consultation Paper on Regulatory Framework for Over-The-Top (OTT) Communication Services, 2018, TRAI highlighted that the “growth in OTT services and the consequent increase in data traffic is also growth for TSP’s business.” The Esya Report cited in this Consultation Paper also indicates that OTT apps boost demand for network capacity, thereby increasing revenue for TSPs. Additionally, in a October 2022 paper titled, ‘BEREC preliminary assessment of the underlying assumptions of payments from large CAPs [content and application providers] to ISPs’, BEREC found no evidence of free riding and noted that 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).<sup>4</sup>

Moreover, there is no need for economic regulation of OTT services as the sector is highly competitive. Creating additional regulations for OTT platforms would be contrary to user interests. Any additional compliance costs arising from increased regulation will end up being passed down to the 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.

The app based economy has significantly contributed to India’s digital transformation and will play a critical role in meeting the Government’s goal of transforming India into a USD 1 trillion digital economy. Therefore, overregulation should be avoided to ensure continued innovation and to support the growth of India’s digital economy and start-up ecosystem.

**Security, Privacy and Safety Aspects:** As stated above, OTTs are well-regulated in terms of data security and privacy under the existing laws such as the IT Act and rules thereunder. OTT platforms are already subject to a range of rules related to cybersecurity, lawful interception, data privacy, intermediary liability, encryption, etc.

There are several provisions under existing law that prescribe privacy and security procedures for OTTs. For instance, the SPDI Rules under the IT Act provide specific privacy related compliances, including the requirement to: (i) provide a clear and easily accessible privacy policy for personal or sensitive personal data being processed; (ii) obtain informed consent for the collection and use of sensitive personal data; (iii) designate a grievance officer for redressal of user grievances within specific timelines; (iv) adhere to data minimization and retention requirements. Such compliances will be covered under the DPDP Act as well.

In terms of security, India’s nodal cyber security agency, CERT-In, prescribes cyber security compliances that apply to OTTs. Under the CERT-In Rules, entities are subject to several cyber security compliances including mandatory reporting of cyber security incidents to CERT-In. Existing laws also address security. For instance, section 43A of the IT Act states that a body corporate handling sensitive personal data or information 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.

Additionally, OTT platforms typically incorporate robust security features to their applications. Some employ strong end-to-end encryption (E2EE) protocols, while others have adopted methods like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman). When it comes to communication features, these are used by OTTs to safeguard user data and messages from

---

<sup>4</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%20%2822%29%20137%20BEREC\\_preliminary-assessment-payments-CAPs-to-ISPs\\_0.pdf](https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%20%2822%29%20137%20BEREC_preliminary-assessment-payments-CAPs-to-ISPs_0.pdf).

unauthorized access, and enable secure communication. To provide a safe and secure experience for users, several OTT platforms have incorporated two-step verifications, options to block or report other user accounts, and privacy controls for users. 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, etc. (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). Moreover, most OTT service providers operate in multiple jurisdictions across the world, are subject to varying degrees of obligations and are scrutinized by agencies across the world. As such, their security and privacy policies in place are generally of internationally accepted standards.

OTT services are also likely to be governed by the upcoming DIA, which will prioritise online trust and safety.

**Quality of Service Aspects and Consumer Grievance Redressal:** As OTTs operate on the application layer, their quality of service (QoS) is largely dependent on the underlying network infrastructure. While the quality of the network infrastructure is regulated by TRAI, other QoS aspects are driven by market forces.

TSPs operate networks, utilize spectrum and facilitate last-mile internet connectivity to users, whether through broadband, wireless, or fixed-line connections. This last-mile infrastructure enables consumers to access OTT and use platforms. 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. Accordingly, building and upgrading networks to provide reliable and high-quality internet access to consumers is a critical compliance obligation for TSPs. Imposing a QoS obligation on OTTs would be ineffective as they typically rely on the infrastructure provided by TSPs and deliver content and services on the application layer over the internet.

OTT services are already incentivized to maintain a high quality of service due to strong competition. Consumers have a range of choices available to them in the OTT market. Switching between OTT services is effortless, merely requiring users to download a new app or explore alternative services on the internet. This high substitutability and the minimal friction involved in the switching process creates a fiercely competitive OTT market. Given the high risk of losing customers, OTTs ensure that maintaining a high QoS continues to remain a priority along with providing mechanisms for consumer grievance redressal.

In the case of paid OTT services, the Consumer Protection Act 2019 allows consumers to file complaints in relation to any deficiency in services, including QoS, payments and misleading advertising. Insofar as OTT service providers are intermediaries, consumers can also report grievances under the IT Rules, 2021. For example, under the IT Rules, 2021, due diligence measures require intermediaries to set up a grievance redressal mechanism, publish the contact information of the grievance officer and redress complaints within prescribed timelines. Moreover, as an industry practice, OTT service providers generally have features such as ‘support chat’ which enable users to directly communicate with grievance redressal teams in real time.

As OTTs operate on the application layer and market forces ensure QoS, there is no requirement to subject OTT service providers to specific or stringent quality of service benchmarks. Existing laws also provide for adequate consumer grievance redressal mechanisms for users of OTTs. Therefore, there is no requirement for imposing separate QoS or consumer redressal obligations on OTTs. Imposing additional obligations may drive up operational costs and limit the ability of OTTs to innovate and test new features.

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.**

**USISPF Response:** There is no need for an additional licensing/regulatory framework for OTTs. OTT services are adequately regulated by existing regulations. **Please refer to our detailed response to (5) above.**

As discussed above, imposing onerous regulatory compliances (typically intended for traditional telecom services) on OTTs will not only adversely impact the ease of doing business in India, but also compel OTT service providers to reconsider their investments in technology innovation and pass on financial burdens to users.

Regulating OTT applications is not only contrary to TRAI's recommendations but is also out of step with international practices. As per ITU: "...New disruptive models of service delivery should not be regulated merely because they threaten an existing model, since such innovation and competition serve consumer interest. Regulators must also be cautious about the impact of their actions on innovation and competition. While important public policy considerations need to be addressed, regulation of OTTs driven solely by the motivation of 'levelling the playing field' between traditional and digital modes of service delivery would be detrimental to consumer interests."

Therefore, as highlighted above, the permission-based licensing regime should only extend to those services which traditionally qualify as 'material resources' and are under the ownership of the government. Bringing OTT services within the regulatory ambit of DOT 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 chilling effect on innovation and investments in the internet ecosystem.

Accordingly, if OTT services are regulated, it will likely: (i) result in unintended regulation of a wide range of unrelated digital services that have no relation to telecom services; (ii) negatively impact the availability of such services due to the higher compliance burden and entry barriers created through regulation; (iii) impede innovation without enhancing consumer protection; and (iv) hamper the development of India's burgeoning start-up ecosystem; and (v) disincentivise foreign investment in India.

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).

**USISPF Response:** We believe that OTT communication services should not be brought under a separate licensing/ regulatory framework. Please see our responses to (5) and (6) above.

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.

AND

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.

**USISPF Response:** There is no requirement to create a formal framework for mandatory collaboration between OTTs and TSPs.

This TRAI Paper cites the ITU's recommendations on 'Collaborative framework for OTTs' highlighting that a collaborative framework may "encourage competition, innovation and investment in the digital economy"; mutual cooperation between OTT service and TSPs to foster "innovative, sustainable, viable business models"; stimulate entrepreneurship and innovation in the "development of telecommunication infrastructures, especially the development of high capacity networks", foster "innovation and investment in OTT services" etc. However, as highlighted in our responses to the questions above, TSPs and OTTs already have a symbiotic relationship as OTT Platforms create value for consumers and drive the demand for internet connectivity services, thus increasing traffic and, revenue of TSPs.

Collaborative frameworks already exist between TSPs and OTT platforms with TSPs and OTTs entering into "*innovative and viable partnerships*" with each other. Moreover, OTT providers contribute to aspects such as infrastructure expansion through the development of Content Delivery Networks (CDNs) and projects to lay deep-sea cables, among others.

A formal framework between TSPs and OTT platforms will be detrimental to the open nature of the internet. Regulatory intervention in the absence of market failure can have negative consequences for both businesses and consumers. Therefore, we recommend that any collaboration between OTTs and TSPs, should be market-driven, organic and voluntary.

## **B. Issues Related to Selective Banning of OTT Services**

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.

**USISPF Response:** The Consultation Paper contemplates selective banning of OTT services or platforms to ensure national security and public order. While these are key priorities, it is important to recognise the adverse impact of selective banning on consumers who have grown to increasingly rely on OTT services. OTT platforms are used for a range of purposes including communication, education, job creation, business, social interaction etc. The growth of the OTT sector has provided opportunities for entrepreneurship, levelled the playing field for businesses, and democratized access to information. The Supreme Court of India has also recognized that the right to freedom of speech and the right to carry on trade and business using the medium of the internet as constitutionally protected rights under Article 19 of the Indian Constitution.<sup>5</sup> Therefore, selective banning should only be undertaken in exceptional circumstances in accordance with existing laws. Any selective banning undertaken by the government should be transparent, proportionate and accountable, and adequate procedural and judicial safeguards should be in place.

---

<sup>5</sup> Anuradha Bhasin v UoI, Writ Petition (Civil) no. 1031 of 2019



Moreover, selective banning presents certain technical challenges, including:

- Selectively banning OTT services may not be the best strategy to counter terrorism or curb misinformation. While the policy intent may be to restrict communications between terrorists and anti-national elements, terrorists that are part of organised crime syndicates typically have multiple technological alternatives to communicate over the internet.<sup>6</sup> Moreover, given the technical complexity and difficulty in carrying out hyper-regional geo-blocking, it may not be possible to implement such measures in a short period of time during times of unrest or of any imminent security concerns. Selective banning may end up adversely impacting users and local communities who wish to access OTT services for legitimate purposes.
- The Department of Telecommunications in 2021, before the Standing Committee on Communications and Information Technology, recognised the challenges of selective blocking. By way of an example, DoT highlighted that “services hosted on cloud are difficult to ban selectively since they operate from multiple locations in multiple countries and continuously shift from one service to the other.”
- For blocking on the application layer, OTT services and websites will require the location information for all users either through GPS data or Cell ID data. If this method is adopted, the GPS locations of users will be continuously tracked, which poses significant privacy concerns.
- Attempts to selectively block information through IP addresses also poses challenges, primarily related to the identification of IP addresses. Sharing of IP addresses by OTT services/websites poses the risk of hacking and denial of service attacks on their infrastructure. Further, technical workarounds such as masking IP addresses or dynamically changing them may prevent effective implementation.

**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.**

**USISPF Response:** There is no need to put in place a framework for selective banning of OTT services/websites under the Telecom Suspension Rules or any other law.

Insofar as the Temporary Suspension Rules are concerned, they are formulated under the Indian Telegraph Act, 1885 and are applicable to ‘telegraph’ as defined under the Act, which does not seek to regulate the application layer services. OTT services would not fall within the definition of “telegraph” or under the scope of this Act.

Moreover, Indian laws have adequate provisions to block online content. For instance, there are existing provisions that enable the blocking of content on recognised grounds. The IT Act and rules thereunder, already contain provisions to address security concerns, including blocking of information in emergency situations under Section 69 of the IT Act. These provisions have also been used to block not only particular content or information, but entire websites and applications on grounds relating to the sovereignty and integrity of India, national security, public order, etc. Similarly, under Section 79 of the IT Act, access to online content can be blocked under certain grounds. This section also allows relevant government agencies to request information from intermediaries for the purpose of identity verification, prevention, detection, etc. of crimes, or for cyber-security incidents. Therefore, there is no requirement for a fresh policy on selective banning of OTT services. Any deficiencies in existing laws may be rectified by strengthening existing legislation, if required.

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

---

<sup>6</sup> Five ways to stay online, Vittoria Elliot, <https://restofworld.org/2022/blackouts-five-ways-to-stay-online/>

- (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.

AND

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.

**USISPF Response:** Please refer to our response to (10) and (11) above.