

From: "yashwanth vankadara2224" <yashwanth.vankadara2224@sidtm.edu.in>
To: "Akhilesh Kumar Trivedi" <advmn@traf.gov.in>
Cc: dydirector@sidtm.edu.in, "ayush sharma2224" <ayush.sharma2224@sidtm.edu.in>, "himanshu maurya2224" <himanshu.maurya2224@sidtm.edu.in>
Sent: Friday, August 18, 2023 5:17:44 PM
Subject: Comments on Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services

Respected Shri Akhilesh Kumar Trivedi, sir,
Greetings of the day!

We are Symbiosis Institute of Digital and Telecom Management (SIDTM), an academic institution based in Pune. We would like to submit our comments on the "Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services"

The comments are attached herewith in PDF format.

Thanks & Regards

Yashwanth Vankadara

Symbiosis Institute of Digital and Telecom Management (SIDTM)

Email: yashwanth.vankadara2224@sidtm.edu.in

Mobile: +91-9866669654

Disclaimer:

This mail is governed by the Disclaimer Terms of SIU, which may be viewed at <http://siu.edu.in/disclaimer.php>

Response to TRAI's Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services

Contribution by:

Ayush Sharma

2nd year MBA (Digital & Telecom)

Symbiosis Institute of Digital and Telecom Management, Pune

Email ID: ayush.sharma2224@sidtm.edu.in

Himanshu Maurya

2nd year MBA (Digital & Telecom)

Symbiosis Institute of Digital and Telecom Management, Pune

Email ID: himanshu.maurya2224@sidtm.edu.in

Yashwanth Vankadara

2nd year MBA (Digital & Telecom)

Symbiosis Institute of Digital and Telecom Management, Pune

Email ID: yashwanth.vankadara2224@sidtm.edu.in

Under the guidance of

Prof Giri Gundu Hallur,

Associate Professor,

Symbiosis Institute of Digital and Telecom Management, Pune

Email ID: girihallur@sidtm.edu.in

About the Institute

SIDTM, in its 27th year of existence, is a constituent of Symbiosis International University, is the first institute to offer management training in digital, telecommunications, and information technology. It is a unique curriculum that combines Digital & Telecom Technology with Management, and it was founded in 1996; by the honorable Dr. S.B. Mujumdar sir (Chancellor of SIU), who took a bold stride forward. In the entire SAARC area, SIDTM is the premier institution for MBA in Digital and Telecom programs, with ranks of Best Telecom B-School in the specialty sector.

SIDTM is dedicated to training world-class ICT Business Leaders who can successfully manage the dynamic and ever-changing technical and business paradigms with ease and expertise. SIDTM helps attract brighter minds by providing them with opportunities for healthy growth throughout time, resulting in well-disciplined and optimistic Techno managers. Technology affects all business models, so SITDM is becoming more relevant and will become an institute of great importance in the future.

Acknowledgements

Symbiosis Institute of Digital and Telecom Management (SIDTM) would like to express sincere gratitude to the Telecom Regulatory Authority of India, for addressing the concerns related to OTT Regulation and Selective Banning. We resonate with the authority's interests of national security and believe it is something that is the need of the hour. Combined with the young talent that SIDTM fosters, and the academic expertise held at the institute, we would like to put forth our comments on the matter at hand. The rest of the paper discusses the same.

A. Issues Related to Regulatory Mechanism for OTT Communication Services

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

Response:

OTTs can be defined as a range of services, including messaging services, voice services (VoIP), and TV content services (Ofcom, 2015). OTT services can also be defined as best effort digital communications services provided over an Internet connection, where calls and messages being routed in the same way as other Internet traffic (Ofcom, 2015). OTT video services can be defined as audiovisual content delivered on the Internet rather than over a managed IPTV architecture (Ofcom, 2018).

“OTT services are broadly defined as any digital communication service(s) that is/are similar to and offer alternatives to services for which Telecom, Broadcasting or Payment Service Providers are licensed and/or collect, store & use end-user data.”

In our opinion, the above-mentioned definition covers all aspects of present as well as future OTT services. This definition covers all the current services such as Calling, messaging, audio-video conferencing, broadcasting services and payment banks and e-wallets for which license is provided by DoT, I & B Ministry or the RBI.

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

Response:

We agree with the Commonwealth Telecommunications Organization Report 2020 on OTTs. OTTs can be classified into four types

(1) OTT-Digital Communication Services (OTT-DCS-NI) (Number independent) apps such as Skype help users to make VoIP calls to PSTN and Mobile Networks. Apps that help users to make calls, messaging over the public internet amongst their subscribers, Google Meet, Discord, Snapchat also fall into this category.

(2) OTT-IP-ND (number dependent) Service Providers that help users to make calls, messaging over the public internet amongst their subscribers . Apps such as Viber, WhatsApp, Facetime fall in this category.

(3) OTT-Content those service providers that potentially compete with broadcasting services by offering Video and Audio content over the internet e.g., YouTube, Netflix, Amazon Prime, Pandora, Google Music, Apple Music, Spotify etc.

(4) OTT-Other apps that offer social networking, e-wallets, ecommerce, that neither compete with electronic communication services nor broadcasting services. Apps such as Facebook, Instagram, Amazon, Amazon Pay, PayTM, fall into this category (CTO Over-The-Top (OTT) Report, 2020).

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

Response:

“OTT services are broadly defined as any digital communication service(s) that is/are similar to and offer alternatives to services for which Telecom, Broadcasting or Payment Service Providers are licensed and/or collect, store & use end-user data.”

In our opinion, this definition of the OTT is broad enough to accommodate existing as well as future OTT services.

We agree with the OTT characteristics stated by SOUTH ASIAN TELECOMMUNICATIONS REGULATOR’S COUNCIL (SATRC) in their 2016 report on OTT.

The OTT services can be characterized as:

(1) Real-time OTT application and services or Communication Services (Voice, Video and Messaging)

(2) Non-real time OTT applications and services (Social networking apps, e-commerce, Cloud storage, e-health, e-education apps etc.)

These characteristics will help the regulators and policy makers in categorizing apps and ensuring their registration in the appropriate category. This will also help regulators to identify OTT apps that fall in the jurisdiction of the sector regulators as well as the regulations that apply to them. For e.g., Voice, Video and messaging OTT services will fall under the gambit of DoT, Video OTTs will fall under the gambit of I&B ministry similarly e-commerce will follow RBI guidelines.

Q4: What could be the reasonable classification of OTT communication services based on an intelligible differentia? Please provide a list of the categories of OTT communication services based on such classification. Kindly provide a detailed response with justification.

Response:

We agree with the Commonwealth Telecommunications Organization Report 2020 on OTTs. OTTs can be classified into four types

(1) OTT-Digital Communication Services (OTT-DCS-NI) (Number independent) apps such as Skype help users to make VoIP calls to PSTN and Mobile Networks. Apps that help users to make calls, messaging over the public internet amongst their subscribers, Google Meet, Discord, Snapchat falls into this category.

(2) OTT-IP-ND (number dependent) Service Providers that help users to make calls, messaging over the public internet amongst their subscribers. Apps such as Viber, WhatsApp, Facetime fall in this category.

(3) OTT-Content those service providers that potentially compete with broadcasting services by offering Video and Audio content over the internet e.g., YouTube, Netflix, Pandora, Google Music, Apple Music, Spotify etc.

(4) OTT-Other apps that offer social networking, e-wallets, ecommerce, that neither compete with electronic communication services nor broadcasting services. Apps such as Facebook, Instagram, Amazon, Amazon Pay, PayTM, fall into this category (CTO Over-The-Top (OTT) Report, 2020).

These categorizations will help the regulators and policy makers in categorizing apps and ensuring their registration in the appropriate category. This will also help regulators to

identify OTT apps that fall in the jurisdiction of the sector regulators as well as the regulations that apply to them. For e.g., Voice, Video and messaging OTT services will fall under the gambit of DoT, Video OTTs will fall under the gambit of I&B ministry similarly e-commerce will follow RBI guidelines.

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

Response:

The TRAI in this consultation paper has brought out an important observation that OTTs have had a positive financial impact on the telecom sector with revenue from data usage rising from a meagre 8% to a dominant 85% as a percentage of total revenue and this trend is mirrored in the ARPU. So, in our opinion, the OTT industry is contributing very well in attracting and retaining telecom subscribers through a variety of attributes such as new and innovative genre of content, personalization and lower tariffs for content as compared to traditional broadcasters.

We agree with approach taken by European Union which states the key areas where OTT needs to be regulated are:

(c) **Security aspects:** these include both personal as well as national security. In this context, we suggest that all OTTs that want to operate in India should mandatorily register themselves with the DoT. It should be mandatory to have a data center in India and guarantee support to law enforcement agencies in case of national security issues.

(d) **Privacy aspects:** all OTTs that want to operate in India should mandatorily register themselves with the DoT and should mandatorily abide by the Personal Data Protection Law in India.

(e) **Safety aspects:** all OTTs that want to operate in India should mandatorily register themselves with the DoT and should mandatorily follow the content regulations and guidelines given by I & B Ministry . The current system of categorization of content as per age groups should be continued with. In case where content is being consumed by minors, consent by elders should be made mandatory.

(f) **Consumer grievance redressal aspects:** The various categories of OTT service providers follow the following mechanisms for redressal of consumer complaints.

- Social Media- Grievance Appellate Committees (GACs) appointed by the Indian government
- Online news - News Broadcasters & Digital Standard Authority (NBDSA).
- OTT Video- Digital Publisher Content Grievances Council (DPCGC) set up by Internet and Mobile Association of India (IAMAI) is a self-regulatory body for Online Curated Content (OCC) providers.
- OTT Messaging- Appointment of grievance officer as per new IT rules by Government of India.

Several countries have supported studies to study the impact of taxation on OTT. Some have gone ahead and introduced taxation on OTT. A study done by Research ICT Solutions and Alliance for Affordable Internet (A4AI) in Benin found that such taxes would decrease broadband adoption, broadband usage and operator revenues, and that the cost of implementing the taxes would be too high.

So, in our opinion, OTT services should not be subjected to financial conditions or licensing or associated regulatory filings. A nominal one-time registration fee to be paid to DoT can be levied. However, in areas of lawful interception; privacy and security and consumer grievance redressal, OTT services should be mandated to follow the self-regulatory mechanisms mentioned above.

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

Response:

In our opinion, there is no need to bring OTT services under financial conditions or licensing or associated regulatory filings. A nominal one-time registration fee to be paid to DoT can be levied. However, in areas of lawful interception; privacy and security and consumer grievance

redressal, OTT services should be mandated to follow the self-regulatory mechanisms mentioned above.

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

Response:

According to an ITU 2020 report, collaborative opportunities exist between OTT providers and TSPs, given that most TSPs have turned to data-centric business models. The ITU study report noted that this shift has resulted in benefits such as reduced churn rates, increased net promoter scores, more stable in-bundle revenue streams, and the ability to link returns more directly to network investment (ITU, 2020). Thus, a TSP/OTT collaboration may offer a mutually beneficial solution, resulting in increased revenues and improved market positioning for both parties due to the enhanced quality provided to customers. Further, in the Indian context, such collaborations are operational in the form of bundled tariff plans as part of which subscribers get access to OTT content. This arrangement is entirely market driven and is currently working perfectly.

So, in our opinion, there is no need for a regulator - initiated /monitored collaborative framework between OTT and TSP's. However, the TRAI/Competition Commission of India may be requested to intervene in any violation of net neutrality principles or in the use of anti-competitive behavior.

This is the end of Part A of the consultation paper. Below is our comment on Part B of the consultation paper, which is about Selective Banning of OTT.

B. Issues Related to Selective Banning of OTT Services

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

Response:

There are several challenges identified concerning to selective banning of OTT services and websites in specific regions of the country for a specific period. The challenge and the proposed solution are addressed below.

Challenge 1: Cloud-Hosted Applications

Applications that are hosted on platforms such as Amazon Web Services and/or Microsoft Azure have an approach different from the conventional method for application and/or website deployment. From the technical perspective, all the applications/websites are accessed from API, and they, by definition, do not have any IP address allocated to them. All services are navigated through Route 53 of AWS for AWS applications which is a DNS service provided by AWS.

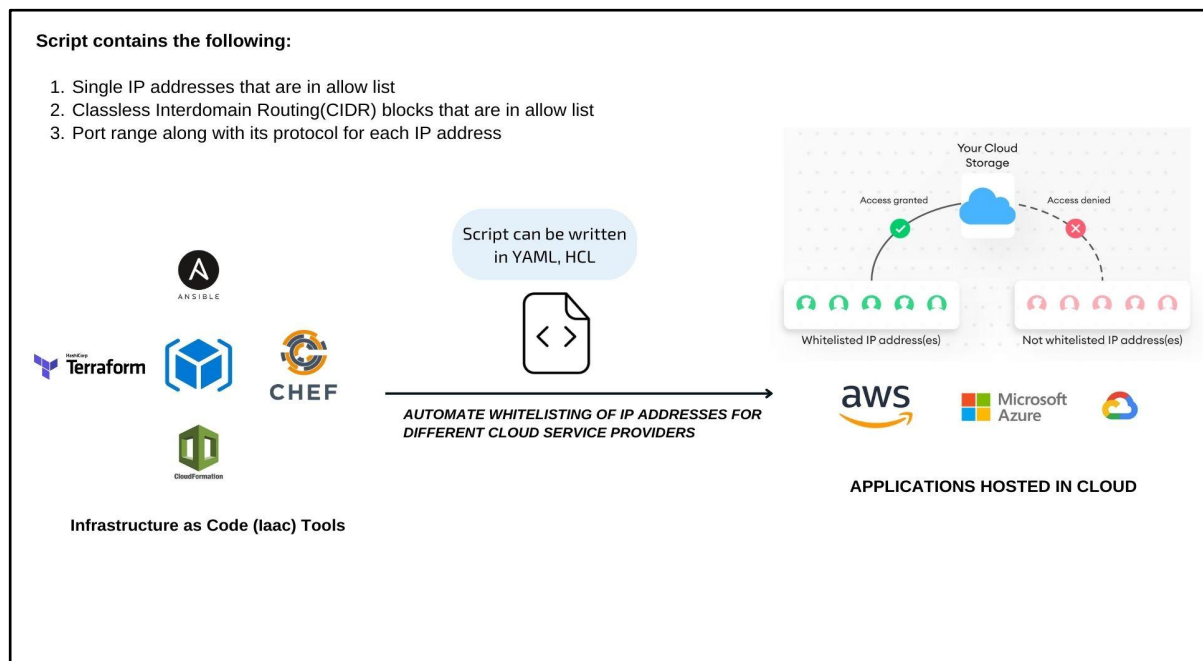
Most of the firewalls are designed to block traffic based on IP addresses. And blocking services solely based on their IP addresses can be challenging due to the changing nature of cloud infrastructures. Cloud service providers use load balancers and virtualization techniques to distribute traffic between multiple servers, and the IP address associated with these servers can change frequently. Since the regulatory authority would have difficulty blocking the IP address, blocking websites and applications hosted on the cloud would be difficult.

Solution to the above challenge:

The proposed solution moves from an IP-based blocking mechanism to a Deep Packet Inspection based approach to block traffic based on keywords. Based on the URL entered, it will be possible to identify that the website belongs on the grey-listed websites list and can be effectively blocked. Some service providers, such as Fortinet, have a service for blocking based on IP and based on keywords as well.

Some firewalls also provide the service of SSL/TLS encryption, which can be used to inspect and decrypt the encrypted traffic.

Example: Infrastructure as Code tools can be used for automating the whitelisting of IPs to the firewalls of different cloud service providers. We can use modules to create and manage IP sets for Web Application Firewall (WAF) rules and Security Groups. We can use HCL (Hashicorp Configuration Language) or YAML (Yet Another Markup Language) to write the script for automating whitelisting of IP addresses.



Challenge 2: Virtual Private Network (VPN)

Virtual Private Network serves as a solution to many problem statements. But, Virtual Private Networks, in general, have a use case, which is of primary concern to the regulators. It allows the users to change their location information to any place in the world, which would mean that the users could be in the location of the riot but claim to be in another city or country and can access the websites/applications that are listed for selective banning. This could be counter-productive to the intention of the regulators who wish to ban OTTs during times of necessity selectively.

Challenge 3: Applications that are not domiciled in India, that is foreign applications.

The impact of this challenge is regarding the processes for obtaining data from the OTT service providers during times of scrutiny. The delay in the process could delay the justice cycle in addressing potential risks.

Challenge 4: Industries like Education, Healthcare, and IT in the region of unrest

The underlying challenge of selectively banning OTT and/or shutting the internet down in the region of unrest is there are institutions like healthcare, educational centers, and IT firms that could belong to the area of unrest, who also depend heavily on OTT services and the internet in general. There has to be a mechanism to ensure that for those entities, it is business as usual.

Solution to the above challenges:

2 solutions can be used to address the above challenges.

Solution 1: Disconnection of primary line and routing traffic to custom-created secondary line.

Long Haul Networks in the country run on various interconnected rings that could be on ADM, MPLS or Carrier Ethernet, etc. technology. All these networks combine short-distance rings that merge with long-haul networks that cover circle after circle.

All these networks have a primary line and also have a secondary redundant line to ensure the availability and reliability parameters of QoS. While most of the traffic majorly flows in the primary line, the redundant path is seldom used, and with newer parameters being introduced, some operators distribute traffic between the primary and secondary lines.

We propose to use this redundant path that can be software configured, to create a model where only the approved applications of the entities that are selectively excluded can run. By doing so, it would be easy for the regulators to follow ahead with the existing solution of the internet shutdown. For the selectively exclusive entities, they would get access to their systems on the secondary line, which is configured to support only allowed applications.

The list of these allowed applications should be priorly disclosed to the nodal offices, and only after formal approval will the applications be listed on Firewall application to ensure that the process can be implemented.

Excluded/Exclusive Entities:

1. IT Companies in the areas of unrest
2. Healthcare providers – Only those above a certain level
3. Education centers with licensed OTT platforms of Zoom/MS Teams/Cisco Webex etc.
4. Data Centers (subject to additional regulations)

Solution 2: Create a network slice of allowable applications on the primary and the other services to disconnect.

The solution revolved around implementing solution 1 on 5G Core.

Solution 3: Telecom Service Providers have a mechanism that allows them to tag every gNodeB with an IP address. This can be leveraged to implement the following:

Identify all the gNodeB in the area of unrest

All telecom service providers already have a DNS server which is used to identify incoming traffic and the end application that is being hit.

At the DNS level, regulators can implement a firewall that ensures that all packets are dropped to the websites that need to be selectively blocked for a specific duration of time (The telcos can also configure their DNS servers at the gNodeB level to resolve the domain names on the list to a predefined IP address that hosts a blocking page or a redirection page).

The issue with VPN will be resolved since the initial data packet has to reach the gNodeB that will make the connection possible. Ingress will be blocked.

Whitelisting of websites and applications will ensure that only the allowed egress traffic can be validated. Since telco handles the mechanism, they are currently equipped to handle it at a specific region level from their OSS.

Q11. Is there a need to put in place a regulatory framework for the 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.

Response:

Yes, there is a need to put in place a framework for the selective banning of OTT services under the Temporary Suspension of Telecom Services. We suggest a “Theatre Command” approach that should work together for the implementation, monitoring, and regulation of OTT selective banning.

The committee will be monitored by TRAI and/or DoT based on the requirement and definition. Still, this committee would have the power to advise for/against the requirement of selective banning of OTTs during the period of unrest.

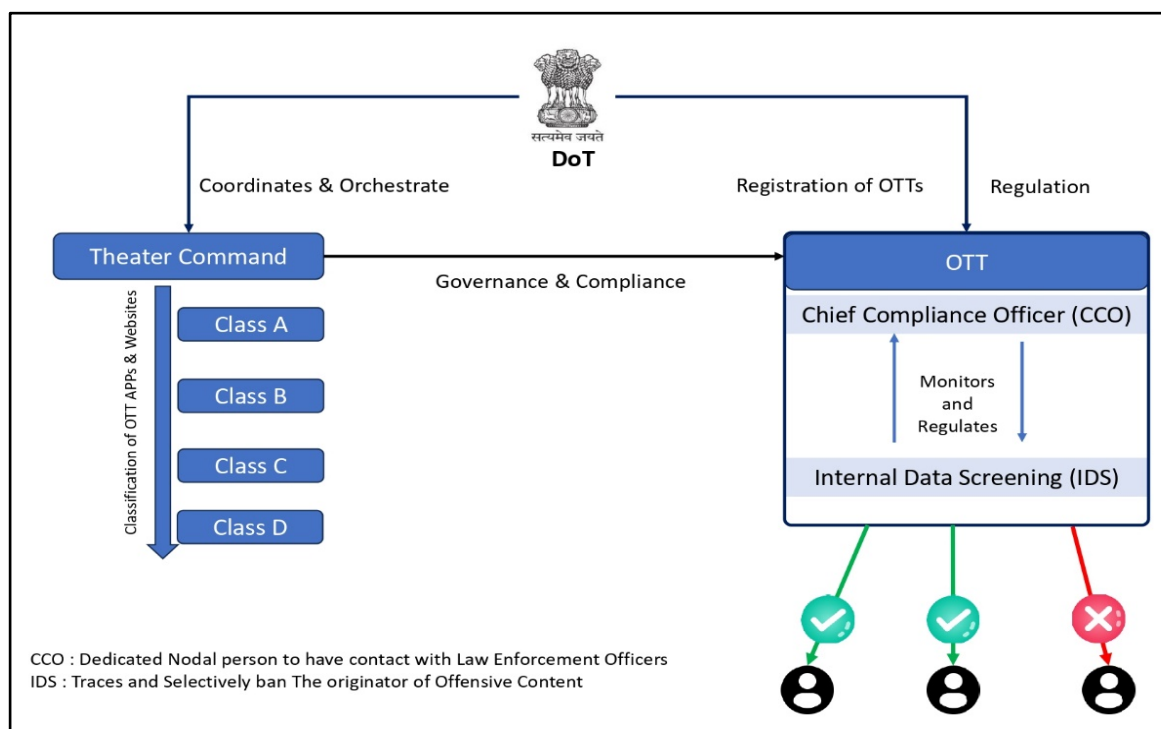
Members of the committee:

1. Member from TRAI, COAI
2. Member from Broadcasting Ministry
3. Member from DoT
4. Member from NIC
5. Member from Government (IB/NIA)
6. Secretary to the Telecom Minister
7. Member from Broadband India Forum
8. Member from DoS
9. Member from NDRF

Functions of the committee:

1. Advisory role to TRAI/DoT for/against selective OTT banning at each requirement
2. Ensuring risk-free implementation
3. Updating database for URLs and IPs of websites that should be selected
4. Redefine the sphere of influence to ensure compliance with third-party integrations
5. Monitoring for Impact
6. Review functions after selective banning is terminated
7. Confirming business as usual after the temporary suspension is revoked

Self-Regulation of OTTs



The proposed self-regulatory structure is in the national interest and will enable DoT to have a Light touch regulation on OTT Platforms.

The DoT forms a Theater Command, classifying OTT Apps and Websites into different classes depending on their services. Services can be Voice, Video, Text/Multimedia messages, Payments, and Media. Other OTT players offer these services and can be classified into classes depending on their severity and reach.

The Classes can have different sets of Restrictions on OTTs which can be imposed in times of unrest. This prevents Governance and compliance with the OTT ecosystem. The OTTs need to appoint a Chief Compliance Officer (CCO), who is the dedicated Nodal person to have contact with Law Enforcement Officers, and he holds the responsibility of the platform contact.

The CCO Regulates the platform's Internal Data Screening (IDS) system and can trace and ban the originator of offensive content.

This selective banning of the User will help to curb the unrest, and other users can use the platform without any disturbance.

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

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

Response:

Different classes of OTT services should be covered under the Selective Banning as A set of services are offered by a single OTT. Ex- WhatsApp offers Voice, Video, Text, Payments, Document sharing, and Location services; identifying them individually and banning them is crucial.

Services are below listed:

- Text / Multimedia Messaging
- Voice
- Video
- Video Streaming/Conferencing
- Payments
- Media
- Location
- Document Sharing

These services can be clubbed under one class, and these classes can be used to put a halt on a few services rather than all.

For example:

Class A- Voice and Text.

Class B - Voice, Text, Video.

Class C- Voice, Text, Video, Video Streaming/Conferencing.

Class D- Voice, Text, Video, Video Streaming/Conferencing, and Media.

Class E- Voice, Text, Video Streaming/Conferencing, Media, and Payments.

Similarly, all the services can be clubbed together to form classes which one selected will stop all the respective services in the particular region for a specific period of time.

Q13. Is there 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.

Response:

All applications and websites that are classified as social media

- Chatrooms in general
- Chatrooms in games
- OTT Communication Services such as Zoom, Google Meet
- Streaming applications like Discord and Twitch
- Blogging websites

Justification:

The main aim of the consultation paper is to ensure that the elements that are involved in creating unrest in a particular region can be curbed. Amongst those elements will be the drivers of the unrest, who would prefer to establish communication via all means to ensure they can share strategies and Modus Operandi in real-time to progress the situation forward. Certain methods through which it can be done are mentioned above.

Special care should be taken for strategy and multiplayer games, such as BGMI, where the entities can create rooms for the purpose of gaming but instead share ideas on how to take the situation to the next stage. Such platforms have been identified in the above-mentioned list.