From: anandpushkar088@gmail.com
To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>
Sent: Thursday, August 31, 2023 6:49:10 PM
Subject: Response to TRAI's paper on Regulation and Selective Banning of OTT Services

Dear sir,

I am writing to you to offer our inputs on the consultation paper on 'Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services' on which comments have been invited till September 01, 2023. I am of the opinion that the current definition of OTT services adopted by TRAI, and as an extension, any classification of such services, will be unable to reflect the complexity arisen by the multiple functions performed by a service. Hence, on principle itself, I hold a preliminary view against the licensing and registration of OTT services. I also believe that in addition to a lack of adequate evidence indicating a need for regulatory intervention, lack of a clear statutory basis or reasoning exists for TRAI to take this matter up for consultation. I am also apprehensive of the approach of selective banning of OTT services, given its ad-hoc, ambiguous, and impractical application, and the negative consequences it may have of user choice and freedom.

Kind Regards,
Pushkar Anand

Detailed submissions on the 'OTT Regulation and Selective Banning' consultation paper

A. Issues Related to Regulatory Mechanism for OTT Communication Services

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

The ambit of this consultation is sought to be limited at the outset with the definition of OTT [Over-The-Top] being narrowly defined by the Consultation Paper. While an OTT service may be any internet application or service which sits on "top" of a telecommunication ("telecom") network, the present consultation limits the scope to only those which, "is accessed and delivered through an application (App) over the public Internet, using the network infrastructure of telecom service providers" and "is a direct technical/ functional substitute for traditional telecommunication services provided by the telecom service providers".

There is some historical baggage to this particular choice. In the previous Net Neutrality and OTT Regulation paper published on March 27, 2015, the Telecom Regulatory Authority of India (TRAI) lacked precision in its argument outlining the regulatory and economic imbalance between TSP and OTT services, and ended up making paternal statements for regulation, citing arguments such as online gaming and social media addiction. This approach seems to be driven by an instinct to regulate the internet per se from the lens of TSPs rather than satisfy any regulatory need. The SaveTheInternet.in campaign also consistently avoided the use of "OTT" in preference to "internet applications and services". To many, "OTT" was a reductionist term which limited the vibrant, innovative pace of applications and services.

In an effort to reach a firmer understanding of the term "OTT", it lists various attempts made to define it by various jurisdictions, forums and international bodies. In this consultation paper, TRAI lists definitions of OTT services published by Organisation for Economic Co-operation and Development (OECD), The Office of Communications (Ofcom), United Kingdom, Body of European Regulators for Electronic Communications (BEREC), etc. There is a problem in this approach as India has adopted an indigenous, progressive approach towards net neutrality which is in many ways due to the leadership of TRAI setting the norms of net neutrality.

Hence, while India may learn from definitions developed in other jurisdictions, we may have an opportunity to help globally set standards once again. Notably, BEREC has also criticised the suggestion to make OTT content providers pay for the rollout of 5G and broadband in Europe and voiced its concerns on whether such a move would help the EU meet its connectivity targets. As per recent reporting, telecom ministers from 18 countries either rejected the proposed network fee levy on tech firms, or demanded a study into the need and impact of such a measure.

One of the criterias used by TRAI to define OTT services in this consultation paper is that they are direct technical/ functional substitutes for traditional telecommunication services. This, according to us, is a very reductive and improper criteria as the substitutability of any service cannot be clearly made out and is closely linked to a large list of criteria. Let us for instance consider internet based calls, in which user behaviour is distinct due to voice quality, reliability and ease. For instance, many use voice calls in preference to data calls and would usually do it for emergency services. We may on the contrary use data calls when the network is spotty or we are talking to a friend abroad. Both services co-exist, for very different purposes. There are inherent structural differences between the two as well, the primary one being that OTT communication services are essentially internet-based apps, which don't own or operate telegraph equipment. Further, OTT communication services do not enjoy exclusive permissions enjoyed by telcos, such as ability to obtain numbering resources, the right of way to set up Infrastructure, etc. Thus, the arguments for substitutability of services between telcos and OTT communication services are unfounded.

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.

Here, our concern is in extension to the one alluded to in our response to the previous question. The current definition of OTT services adopted by TRAI, and as an extension, any classification of such services, will be unable to reflect the complexity arisen by the multiple functions performed by a service. Several internet applications and services offer multiple functionalities— which may include voice calling and instant messaging —even though their primary functionality, for instance, may be social networking. With WebRTC, nearly all browser based content and mobile applications can have a communications layer that supports messages, voice, and video. Will such services also be brought within the regulatory ambit? Furthermore, how will these services be classified as their functions may be cut across several categories.

TRAI lists the classification of OTT services as provided by various jurisdictions and forums. One of these classifications was provided by the Department of Telecommunications ("DoT") in their 'Committee Report on Net Neutrality' published in May 2015, wherein DoT grouped OTT services into OTT communications services (providing realtime person to person telecommunication services) and OTT application services (services such as media, trade, commerce, social media, trade). TRAI lists similar classification attempted by other forums and organisations such as BEREC, Commonwealth Telecommunication Organization, etc. However, what remains unclear is how an OTT service, which provides social networking services and also electronic communication services as a primary and secondary functions respectively, will be categorised.

To us, this is again illustrative of the oversimplification of a debate that commences from dulling the feature richness and diversity of internet applications and services into the straightjacket of OTT. The dangers of avoiding bright lines of regulation and the uncertainty in treatment may prevent free expression which is the very basis for innovative thought and action. There are also concerns that overbearing and costly legal compliances and product decisions which may harm India's vibrant start-up ecosystem. Even a case-by-case assessment may bring in uncertainty and build ad-hocism. Hence, on principle itself, we hold a preliminary view against the functional definitional treatment of internet applications and services as OTTs as well as their categorisation as per the services offered by them which further builds into a case for licensing and registration to protect telecom service providers ("TSPs").

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.

Same response as given for Q1.

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.

Same response as given for Q2.

Please provide your views on the following aspects of OTT communication services vis-à-vis licensed telecommunication services in India:
Regulatory aspects;
Economic aspects;
Security aspects;
Privacy aspects;
Safety aspects;
quality of service aspects;
consumer grievance redressal aspects; and
any other aspects (please specify).
Kindly provide a detailed response with justification.

TRAI lists the obligations applicable to TSPs and the arguments put forth by organisations such as ITU and BEREC on the need (or lack thereof) for developing a policy and regulatory framework for OTT communication services. To substantiate the economic premises put forward by the ITU, TRAI listed some data (declining number of outgoing SMS and international long distance voice minutes of usage, as well as increasing volume of monthly wireless data usage and monthly average revenue per user (ARPU) for wireless subscribers). There are also subsidiary arguments made to further these two premises. These include the rising user consumption of data, the dropping price of data per GB due to competition amongst telcos, growing convergence (where even voice calls originate over data networks), which requires investments for upgradation and increasing the capacity of existing networks. All these trends are stated on the basis of reference to reports by consultancies and industry associations.

We urge TRAI to interrogate the premise, i.e. the existence of service substitutes, in which several internet services are supposedly direct substitutes of traditional services and are thus stealing the latter's revenues and profits as well as the existence of a market failure, in which there is a lack of adequate financial incentive for large telecom players to invest in infrastructure due to the lack of compensation. TRAI, throughout the Consultation Paper, makes this to be the causal link requiring regulatory intervention.

Ideally any prescriptions on this in the consultation paper should commence from a data driven analysis which provides evidence for the revenue losses borne by traditional telecom companies thus impairing future telecom network investment. To fill this gap we conducted an economic analysis of the financials of large telecom players over a 7 year period from 2015, based on their own publicly-available quarter-to-quarter statistics [Link] [See here the data sheet broken across quarters that maps the financials of the sector based of TRAI data, and three large telecom companies, Airtel, VI (Vodafone and Idea), and Reliance Jio]. As such, we determined that three inferences could be made from the data:

Both voice and data usage have seen a significant increase between 15Q2 and 18Q1, i.e. roughly between July 2015 and June 2018, exploding after 16Q2 with the entrance of Reliance Jio into the telecom sector.

This massive growth coincided with a drop in per user revenue for the major telecom players. Such fall appears to be due to a hyper-competitive environment engineered in the sector by the entry of Reliance Jio, however with a wave of consolidation this period may soon end. We also further predicted that with a wave of then-upcoming consolidations (like the merger of Idea and Vodafone), this period of lower revenue streams would

soon end. These trends are as per statements in the press by leading executives of telecom companies and analyst reports such as Moody's and Fitch.

We also noted that while the data displayed a need for continued investment, the extent of the necessary investment was unclear from the data available from the telecom companies. We thus called for a clear, public statement backed with data to be made, if there is truly a need for investment.

What the data thus implies is that an increase in data use - and therefore the services accessed using such data, including the use of OTT communication services like instant messaging or voice and video calling - cannot be blamed for decreasing or negatively affecting revenue streams. Although major telecom companies tend to attribute various factors to this decline, intense competition remains most likely to be the main cause. It is our initial belief that implementing regulations that impose financial burdens or levies on internet platforms and services is not a wise public policy approach. Rather than protecting company profits of both telcos and OTT service providers, the goal of regulation should be to serve the public's best interests.

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.

This is a relevant concern for the Consultation Paper to indicate as the market power of large online platforms concentrates and quite often there is a lack of compatibility or ease of migration from one online service or app to another. This can result in a lock-in for a user to a particular online service provider. While this is a credible public policy concern and may require regulatory intervention, we are unsure whether the TRAI, as a telecom regulator, should be the one to take this up.

Before we deal with issues around TRAI taking up this public policy concern, we must deal with a fundamental question, i.e. whether licensing is an appropriate approach to tackle competition concerns. The aim of licensing is to ensure responsible use of resources that are scarce in nature. This is why the government provides licences for mining operations and electromagnetic spectrum. However, since OTTs are non-scarce and non-rivalrous internet based applications, the rationale for licensing does not apply. Any social or competition concerns that arise out of the use of these apps are/should be tackled already by sectoral legislations such as the Consumer Protection Act, 2019, Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, etc. Further, the Competition Commission of India (CCI), in its report summarising the main findings of the Market Study on the Telecom Sector in India noted that "experts feel a separate regulatory framework is not necessary for OTTs and excessive regulation may stifle technological innovation, and therefore be counterproductive".

An accompanying fundamental problem to ponder over is the effect OTT licensing may have on non-dominant service providers. In a sector where market concentration is likely, the inclusion of a non-dominant player under the licensing regime may further create barriers for entry into the market and the ease of doing business. Inclusion of OTT players under the regime on an ad-hoc basis, primarily due to the ambiguity around definition and classification of OTT services, may also have negative implications.

In addition to our fundamental concerns with the approach, our other two basic reasons for hesitance are: firstly, the lack of a clear statutory basis to do so (TRAI may go outside its legal mandate by dealing with issues of competition and consumer interest); and secondly, it may turn the TRAI into a regulator for the internet based applications. We believe the absence of legality and authority, even to seek opinion on such matters, would also blur the objectives of regulation and the boundaries within which TRAI would have to restrict itself. We hope that the issue of interoperability is picked up within competition law and consumer protection frameworks, which may be better suited to undertake this task.

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:

lawful interception;
privacy and security;
emergency services;
unsolicited commercial communication;
customer verification;
quality of service;
consumer grievance redressal;
eligibility conditions;
financial conditions (such as application processing fee, entry fee, licence fee, bank guarantees etc.); and
any other aspects (please specify).
Kindly provide a detailed response in respect of each class of OTT communication services with justification.

Lawful interception: This is an incredibly concerning issue, as India's recently enacted data protection law does not put into place any meaningful safeguards against overbroad surveillance. We have been advocating and campaigning for a strong, user centric data privacy law that includes surveillance oversight and reform. The Expert Committee instituted by the Union Government on data protection chaired by Justice Srikrishna acknowledged that current legal provisions and practices on surveillance - including the absence of any judicial oversight - fail to adequately protect our fundamental right to privacy. A line of argument, one we do not agree with, states that any required safeguards have been achieved through technical measures implemented by users -- this principally includes end to end encryption (E2EE). At this juncture, it is necessary to clearly state that lawful interception of messages can only happen by weakening E2EE, bypassing it, or by not encrypting communication altogether. Not only would this force several encrypted messaging platforms to stop providing their services in the country, but it would also result in erosion of trust among users. Global studies have also shown that similar laws which weaken E2EE have resulted in financial losses and hindered economic growth. Given the safety and security afforded to users, businesses, and governments by end-to-end encrypted messaging platforms, we are of the belief that these services must not be compelled to weaken or abandon E2EE. The use of legal or technical means to access data and intercept communications in India must only be authorised only in emergency situations, under judicial control and oversight, and with other protections to safeguard our citizens.

Even though the Digital Personal Data Protection Act (DPDPA), 2023, has been notified the current version lacks a provision on surveillance reform within its ambit or a provision to regulate intelligence and policing agencies, which are the principal recipients of such information. Hence, any conversation which progresses to argue for expanding the applicability of lawful interception, that too in the absence of relevant safeguards, is completely against user interest and will be another step in building a surveillance state.

Privacy and Security: We do not dispute the line of thought that internet platforms and services need to be governed appropriately when a clear social need arises in a rights respecting framework and pursuant to legality. Although India now has a notified data protection law, risks to privacy/security due to interception still exist as the law does not include any safeguards against overbroad surveillance. As we have stated previously, any attempts to intercept communication and weaken E2EE will lead to the erosion of trust, safety, and security of users. Also as indicated before we are not adverse to examination of large social media platforms or data driven businesses within consumer protection and competition law frameworks. However, as we have stated before, this examination must be undertaken by the relevant authorities and not by TRAI.

Emergency services: We have in the past held a view that the conversation regarding this may be deferred to a later date. We believe we have not yet reached the moment for regulatory intervention, but we do hope that better citizen advocacy and user demand spur market mechanisms that may require application providers of internet applications and services to clearly mark that they do not have the functionality for emergency calling. Some other services may by themselves opt-in and offer this feature to users as a product feature. But, the primary point which needs to be stressed is that voice calling and SMS messaging by itself still persists and is a feature which is always available on feature- and smartphones. Hence, emergency services are at present available to users in India to an extent where a regulatory intervention may not be justified.

Unsolicited commercial communications and customer verification: On November 29, 2022, the TRAI released a consultation paper titled 'Consultation Paper on Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks', wherein a proposal for the introduction of CNAP in India was floated. As per the CNAP proposal, the information of a caller would be provided to the receiver, thus giving the consumer the right to make an informed choice as to whether to take the call or not. This proposal was suggested to contain prevalence of robocalls (automated calls used to dupe consumers financially), spam calls (unsolicited marketing calls that bypass the do-not-disturb feature), and fraudulent calls that may obtain details of bank accounts or OTPs with an aim to defraud consumers.

On September 21, 2022, the Department of Telecommunications ("DoT") released the draft Indian Telecommunication Bill ("Telecom Bill"), 2022 for public consultation. Clause 4(7) of the Bill requires every entity receiving a licence to "unequivocally identify the person to whom it provides services, through a verifiable mode of identification as may be prescribed." The "verifiable mode of identification" remains unknown as of now, but what is known with certainty is that the identity of the person receiving the service will have to be established, with complete assurance, by the service provider. Additionally, as per Clause 4(8), the identity of the sender of a message using telecommunication services "shall be available to the user receiving such message, in such form as may be prescribed, unless specified otherwise by the Central [Union] Government". In the explanatory note, the government notes that these provisions are "important to prevent cyber frauds".

While the recognition and acknowledgement of a need to tackle increasing cyber frauds in India is appreciable, potential excessive data collection and retention by several entities raises concerns. These provisions essentially strip away the user's right to stay anonymous while communicating, both offline and online. This can have a deleterious impact on vulnerable individuals such as whistleblowers, who wish to keep their identity anonymous. Services such as Twitter and Instagram, which provided users with the option to communicate anonymously, will possibly have to take back this facility if they wish to operate in India.
Although a data protection law has now been notified, there is still some ambiguity with respect to a user's ability to de-list themselves in case they don't wish their details to be revealed to receivers of messages. Similar ambiguity exists on the ability of the users to get their data deleted, erased, and forgotten. While the DPDPA, 2023 does not include the 'right to be forgotten', the Minister of IT claims that this right has been subsumed under the right to erasure. This conflation between the general right to erasure with the right to be forgotten, which is specific to disclosure of personal data, leads to ambiguity. The mention of right to erasure is also limited by the need to retain information for "compliance with any law for the time being in force" [Section 12(3)] - which when combined with various sectoral/ other data retention requirements, may result in heavy dilution of this right. Moreover, Section 17(3) also includes an exemption from Clause 8(7) which obliges a fiduciary to erase personal data/ ask a data processor to erase it once consent is withdrawn (and the purpose is served). Thus, any and all provisions of the Act must be read with and in context of the exemption provisions as well as other broad qualifiers.
Moreover, given the inadequate safeguards that currently exist for users to avail in case of violation of their fundamental rights, such overbroad requirements must be reconsidered. Given these grave concerns, any measure adopted or suggested by TRAI for verification of customer identity or any efforts to tackle spam calls must not lead to weakening of the user's right to privacy and as an extension, right to anonymity.
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.

It bears repetition that the core thesis of a market failure and the need to correct regulatory imbalances is yet to be established, contrary to our economic analysis that shows that the economic stress is due to a period of hyper-competitiveness. We even dispute the arguments for substitutability of services between telcos and internet applications and services. Thus, we reiterate our stance that there is inadequate evidence at the moment, and therefore no need, for creating a collaborative framework between OTT communication service providers and the licensed telecommunication service providers.

TRAI, in this consultation paper, lists the recommendations given by International Telecommunication Union (ITU) on 'Collaborative framework for OTTs'. The "collaborative framework" recommended by the ITU needs to be read with its accompanying introduction, which reads as follows:

"Consideration of the economic impact of OTTs should be based upon recognition of the fundamental differences between traditional telecommunication operators and OTTs, including inter alia, control of broadband Internet access, level of regulatory exposure, barriers to entry, competitive environment, level of substitutability between OTTs and traditional telecom services and interconnection to public networks. In particular, determination of competitive scenarios involving OTTs and traditional telecommunication services should consider the complexity of their interrelationship. In some cases, they may deliver similar functionalities, in other areas they may be supplementary, whereas in other aspects, OTT may exceed what traditional telecom services typically deliver. Moreover, the advancement in the telecom network catalysed the OTT development, further extending consumer benefits. To continue the momentum in development, competition, innovation and investment need to be encouraged to foster the growth of the entities in the ecosystem, including network operators and providers of OTTs."

Thus, the adoption of any framework must be preceded with an understanding and analysis of the complex relationship and the fundamental differences between the OTT services and TSPs.

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.

As part of our comments dated January 07, 2019, and counter comments dated January 21, 2020 on the consultation paper on 'Regulatory Framework for Over-The-Top (OTT) communication Services' released by TRAI in 2018, we urged TRAI to prioritise users interest and choice, over that of telcos and OTT service providers. We submitted that the paper set multiple faulty premises to pose queries and was thereby representative of inaccurate information, which may lead to problematic regulations. We called for legislative action and regulatory reform in the domains of privacy, consumer protection, and competition law frameworks. We also highlighted that TRAI's consultation queries fell outside the jurisdictional scope of telecom regulation, and thus outside of TRAI's.

B.Issues Related to Selective Banning of OTT Services

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

No response.

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.

Highlighting the high economic and social cost of complete internet shutdowns, TRAI is seeking comments on an alternative approach, i.e. to selective banning of specific OTT applications and websites etc. in specific regions, "which are likely to be used by the terrorists or anti-national elements". The Standing Committee on Communication and Information Technology in its 2021 report on 'Suspension of telecom services/internet and its impact' recommended that the DoT examine TRAI's recommendation and develop a policy to selectively ban OTT services with suitable technological interventions. Similar approach of 'whitelisting'/'allowlisting' some services has earlier played out in Jammu and Kashmir in 2020. Here, some questions arise with respect to the technical ability to implement and overall efficiency of such bans.

What processes and criteria will be applied to select and reject specific URLs/ services/ websites for banning? Will all services providing similar or comparable services be banned or will that decision be taken on a case-to-case basis. The latter may lead to ad-hocism, impose compliance burden on MSMEs, and negatively impact user experience as well as choice.

The Jammu and Kashmir allowlisting order also stated that "The ISPs shall be responsible for ensuring that access is allowed to whitelisted sites only". In the case of the entries that contain neither URLs nor qualifying information about including subdomains or about permitting mobile applications, it should not be left to the discretion of an Internet Service Provider (ISP) to determine the appropriate URLs or the appropriate mode of access (mobile or desktop application, mobile or desktop version) of a allowlisted service or website. ISPs are intermediaries and are not authorised to take a judgement call on the orders they receive from the government. Actions to be taken by an intermediary in case of invalid or indeterminate URLs may also be unclear, leading to ambiguity around how allowlisted entries are to be implemented. Another concern that was witnessed in the Jammu and Kashmir allowlisting order was how the residents were informed of the services that had been made accessible. It is worth noting that these orders appeared in an issue of the gazette, which may not be accessible by everybody.

A paper published by researchers at the Centre for Internet and Society found that different ISPs deployed different techniques for banning services. It also found that less than 30% blocked URLs were common across the ISPs. Such inconsistencies may lead to users having limited to no recourse due to the ISP's lack of accountability and transparency. The ability to make arbitrary decisions regarding accepting/ rejecting the request to ban certain services along with deploying their own techniques to ban services may lead to inconsistent and ad-hoc application.

What also remains uncertain are the methods through which a selective ban will be implemented. Will the ban be limited according to duration of ban or geographical area of ban? A concern worth noting is will the availability of a "restricted shutdown" be misused and lead to more number of shutdowns being ordered, just because they are perceived to be "limited in their impact"? Or will the ban be restricted according to the access to medium (wired or wireless connections)? In this case, will the Union or state authority take into consideration the prevalent digital divide in the country as well as the fact that a minority in the country have wired connections. Notably, while 96.13% of the population have wireless mobile connections, only 3.74% of the population have wired connections.

Other concerns include the impact of banning multi-purpose OTT communication services, such as WhatsApp which is used for communication, payments, and to conduct business. Although the intention to ban may be to curb communication through an app in an area, it may have the unintended consequence of introducing barriers in conducting payments and business. For instance, small-scale businesses with a predominant social media presence faced difficulties in performing business and receiving payments when WhatsApp faced a six-hour long outage in October 2021. It is also unclear if the Union Government will take into consideration a hierarchy of apps while considering banning, i.e. whether to ban an app that occupies most of the internet traffic online by providing multiple online services as compared to another app providing a single service. As per the orders laid down by the court in the Anuradha Bhasin v. Union of India and Ors Judgement, the government would have to comply with tests of proportionality and of least intrusive methods of imposing a restriction.
On July 25, the government of Manipur marginally lifted the internet shutdown. The order allowed restoration of the internet for broadband users (Internet leased line and fibre to the home) subject to several "impractical" conditions. These partial lifting of the internet suspension was made subject to fulfilment of the following terms and conditions:

a) Connection will be only through static IP and that the subscriber concerned shall not accept any other connection other than allowed for the time being [TSP/ISP shall be held responsible for non-compliance of this condition];
b) No Wifi Hotspots shall be allowed from any of the routers and systems using the connection at any cost by the subscriber concerned;

c) Media Access Control Address (MAC) binding at the system level or router shall be ensured with the help of ISP/TSP concerned;
d) Blocking of social media websites and VPNS at the local level will be ensured by the subscriber concerned;
e) Shall have to ensure removal of any existing VPNs softwares from the system and not to install any new softwares/ VPN App by the subscriber concerned;
f) Enforcing Physical Monitoring by subscriber concerned/the concerned authority/officials of checking violation of the terms and conditions specified;
g) Changing of log in ID and Password for respective system on daily basis; and
h) Will obey all orders/ Regulations regarding any change in the condition under which service is being allowed issued by the State Government from time to time by the subscriber concerned.
i) Further, in the event of any violation, subscriber concerned will be liable to be punished as per provisions of relevant laws of the land in force and that I also agree to be fixed personally responsible for any leakage/ activities done by any Secondary user of internet, In case Wifi/ Hotspot had been activated without approval of Home Department from my system/router.
j) ISP shall ensure to obtain undertaking to the extent as explained above before giving any internet connection in the prescribed format (enclosed herewith) without fail.

The order requires users to have static IP connections with system-level MAC binding of devices which allows for precise geolocating of the users. This effectively does not provide any relief to the large population of Manipur, and only helps a negligible section of users with broadband connections and a static IP. According to the Indian Express, "Mac-binding essentially means binding together the MAC and IP addresses, so that all requests from that IP address are served only by the computer having that particular MAC address. In effect, it means that if the IP address or the MAC address changes, the device can no longer access the Internet. Also, monitoring authorities can trace the specific system from which a particular online activity was carried out." This sort of monitoring is extremely worrisome, especially given the hostile environment prevailing in areas under an internet suspension order. Moreover, the requirement on the user to block access to social media websites and VPN services, and to ensure that no wifi hotspots are allowed from the routers or systems using the connection effectively shifts the burden/ responsibility to an individual subscriber. The enforcement of physical monitoring by subscribers or the concerned authority is an example of how the implementation of this order and adherence with conditions at scale becomes impractical. The order worryingly holds the individual subscriber liable for punishment for not just the violation of the aforementioned conditions, but also for the actions of a secondary user of the internet. Thus, the Manipur order is a testament to the fact that a restricted shutdown is impractical and may lead to increased burden, cost, and worrying consequences for subscribers.

We understand TRAI's temptation to consider selective banning over complete internet shutdowns. However the technicalities of implementing such selective bans as well as their effectiveness, must be examined before putting forth this proposal. To date, there has not been any demonstration of the perceived effectiveness of blanket internet restrictions either. We advise against using such means in the name of perceived benefits, especially when evidence exists to portray the real harms.

In case it is decided to put in place a regulatory framework for selective banning of OTT services in the country, Which class(es) of OTT services should be covered under selective banning of OTT services? Please provide a detailed response with justification and illustrations.
What should be the provisions and mechanism for such a regulatory framework? Kindly provide a detailed response with justification.

As we have stated previously, we are of the opinion that 'selective banning' as a concept is extremely concerning and may lead to several unintended consequences. It is worth considering that while malicious actors may find workarounds, citizens that rely on a daily basis on services using the internet at scale may not, and thus will be impacted. Alternatively, those seeking workarounds without any malintent may be also be criminalised. Workarounds may include using alternate applications - which may then prompt the government to continuously expand the list of banned/ blocked applications. It may also include the use of means to proxy/route connections (such as VPNs), ordering restrictions on which would be disproportionate and implementation of which would be challenging, requiring onerous, unimplementable orders like the Manipur order. The use of VPNs, even for

legitimate uses, may result in criminal liability. Thus, we would like to reiterate our apprehension against selective banning and would urge TRAI to issue a recommendation against the framework.

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.

Same response as given for Q11.

Are there any other relevant issues or suggestions related to regulatory mechanism for OTT communication services, and selective banning of OTT services? Please provide a detailed explanation and justification for any such concerns or suggestions.

Same response as given for Q11 and 12.