Mozilla Headquarters
331 E Evelyn Avenue
Mountain View, CA 94041
United States of America
650.903.0800

To:
Shri RS Sharma
Chairman, Telecom Regulatory Authority of India

Shri Sunil Bajpai
Principal Advisor (CA, QOS, IT), Telecom Regulatory Authority of India

Shri Asit Kadayan
Advisor (QOS), Telecom Regulatory Authority of India

RE: Comments of the Mozilla Corporation on the Telecom Regulatory Authority of India's Consultation Paper on Regulatory Framework for Communication OTT services

Dear Sirs,

Thank you for this opportunity to provide comment and input on this Consultation Paper on the Regulatory Framework for communications OTT services.

We commend TRAI for the thoughtful and considered treatment of this topic. We had previously submitted our views to the Authority and the Department of Telecommunications on the potential of a licensing framework for OTT services. We welcome the intent behind narrowing the scope of this enquiry considerably since its previous iteration in 2015, and have put forth our views on the more specific questions posed by the Authority in this consultation.

The Mozilla Corporation produces the Firefox web browser and the family of Firefox products, including Firefox Focus and Firefox Lite, as well as the Pocket, used by hundreds of millions of individual internet users around the world. Mozilla is also a foundation that focuses on fueling the movement for a healthy internet. Finally, Mozilla is a global community of technologists, thinkers, and builders, including thousands of contributors and developers who work together to keep the internet alive and accessible.

If you have any questions about our submission or if we can provide any additional information that would be helpful as you continue your important work, please do not hesitate to contact Mozilla's Policy Advisor Amba Kak at amba@mozilla.com.

Q. 1. Which service(s) when provided by the OTT service provider(s) should be regarded as the same or similar to service(s)being provided by the TSPs. Please list all such OTT services with descriptions comparing it with services being provided by TSPs.

Q. 2. Should substitutability be treated as the primary criterion for comparison of regulatory or licensing norms applicable to TSPs and OTT service providers? Please suggest factors or aspects, with justification, which should be considered to identify and discover the extent of substitutability.

At the outset, we would note that these questions are based on the assumption that there are good reasons to impose a uniform regulatory framework across (communication) OTT providers and TSPs. However, at present we do not see a compelling case for such harmonization and, on the contrary, we think such an exercise may create legal uncertainty, chill innovation, undermine security best practices, and eventually, hurt the promise of Digital India. In May 2015, the Indian Department of Telecommunications' (DOT) looked into this issue and concluded that, "For OTT application services, there is no case for prescribing regulatory oversight similar to conventional communication services."[1] We would strongly urge the Authority to reach a similar conclusion in the specific context of communications OTTs as well.

At present, the Authority outlines three broad potential justifications for regulatory parity: economic impact of OTTs on network infrastructure; interoperability; and data protection and privacy. On economic impact, we argue below that this empirical claim lacks sound economic analysis and moreover, ignores the virtuous cycle between demand for OTT services and revenue generation for TSPs. On the other issues of interoperability and privacy requirements, we think these are critical issues but would be best dealt with holistically in terms of the problem sought to be addressed rather than narrowly focussed on OTT providers or in terms of parity with regulations that apply to TSPs. We address this in depth in our answers below.

Overall, therefore, we see no compelling justifications for creating additional regulatory parity between OTTs and TSPs, nor any need to determine such standard of comparison. That said, on the specific question of definitions asked in Q1, we would also point to certain flaws in the *"same of similar service(s) being provided by TSPs"* standard mooted by the Authority. The definition hinges on the *entities* providing personal communication services, rather than the function itself. For example, as TSPs

[1] http://www.dot.gov.in/sites/default/files/Net_Neutrality_Committee_report%20%281%29_0.pdf at p.86.

today expand into wider service offerings -- for example, entertainment services or news services -- then, in turn, this would expand the scope of any policy to the vast number of OTTs that provide these non-communication services as well.

While TRAI rightly recognizes that TSPs and OTTs deliver calling and messaging services using vastly different technical mechanisms and infrastructure, there are also important economic differences between these types of entities which should be reflected in the regulatory regime. The business models and cost structures of Skype, which offers its calling and messaging services for free and then charges for ancillary services like calling a mobile phone, are substantively distinct from Airtel which pays for an operating license and typically charges consumers directly for calling and messaging services. In order to ensure the orderly growth of the telecom sector and consumer welfare, it is critical for the regulator to heed these crucial differences in business models and technical delivery.

The objective of regulatory parity might also imply (at its extreme) the introduction of licensing or other permission-based frameworks for OTT communications providers. This was mooted in 2015 by the Authority,[2] and Mozilla strongly opposed such a move. As our Executive Chair Mitchell Baker wrote in a letter to Prime Minister Modi[3] at the time, any licensing scheme would prove onerous and *"increase the costs of creating on the Web, thereby discouraging Indian entrepreneurs from building the next Internet giant. What's more, establishing an enabling environment for development on the Web creates a virtuous cycle that provides more value to existing users and incentivizes new users to come online."*

Finally, we would also urge the Authority to note that there are relatively few countries or regions that have introduced (or even debated) the introduction of such an overarching regulatory framework. The European Electronics Communications Code,[4] which has been referred to in this consultation extensively, has since been passed in November and adopted on December 20 2018. As noted by the Authority, the Code does define and categorise OTT providers based on number-based communication OTTs and number-independent communication OTTs (like Skype, Signal or WhatsApp). While the code does bring both these categories of OTTs within regulatory scope, it does not recommend uniform regulations for these distinct entities. Regarding the

[2] https://www.trai.gov.in/consultation-paper-regulatory-framework-over-top-ott-services

[3] https://blog.mozilla.org/netpolicy/files/2015/05/Letter-from-Mozilla-Executive-Chair-Mitchell-Baker-to-Prime-Minister-Modi.pdf

[4] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20181114+ITEMS+DOC+XML+V0//EN&language=EN

application of an authorisation regime on OTTs, they conclude that since such services that don't use public numbering resources nor participate, *"it is therefore not appropriate to subject those types of services to the general authorisation regime."*[5] On security requirements, too, they decide against mandating regulatory parity on the grounds that OTTs *"normally do not exercise actual control over the transmission of signals over networks"* and therefore, "*the measures taken by providers of number-independent interpersonal communications services should be lighter*". [6]

Overall, for number-independent OTTs the European Commission has introduced no major additional requirements, payment or security obligations, nor licensing/authorization regimes for number-independent OTTs. Even on the limited issue of emergency warnings, taking into account technical burdens to implement this measure, implementation for OTTs has been postponed till 2020 when the regulator will reassess whether the penetration rate of these platforms might threaten access to emergency services altogether.[7] We think this is a sound approach, and would urge the TRAI to look to such international precedent that has been concluded after extensive consultations.

Q. 3. Whether regulatory or licensing imbalance is impacting infusion of investments in the telecom networks especially required from time to time for network capacity expansions and technology upgradations? If yes, how OTT service providers may participate in infusing investment in the telecom networks? Please justify your answer with reasons.

At the outset, we would note that this is an empirical enquiry and each stakeholders' claims should be subject to a high degree of scrutiny. It requires evidence of the various factors that can be correlated to the incentives to invest in network infrastructure and the contribution of OTTs themselves to these incentives and to the network infrastructure itself. We submit that accepting one set of stakeholders claims over the other without rigorous scrutiny would lead to poor policy outcomes.

[5] European Electronic Communications Code at s.44, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG&toc=OJ%3AL%3A2018%3A321%3ATOC

[6] European Electronic Communications Code at s.95, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG&toc=OJ%3AL%3A2018%3A321%3ATOC

[7] See https://eena.org/wp-content/uploads/2018/11/European-Calls-EECC.pdf

In general, we agree that investments in telecom networks are critical to increasing the value of the internet and ensuring better speeds and access. However, expecting OTTs to financially contribute or pay TSPs to access users has been globally recognised to be an inefficient economic tool to do that.[8]

For one, there is no clear or necessary connection between transferring finances to TSPs and that being used towards the expansion of network infrastructure. On the other hand, one need only look at the Authority's data[9] which demonstrates that increased demand for data has and will continue to spur network investment. TSPs remain financially healthy and with new entrants like Jio the sector has seen consolidation and overall growth in the number of data customers. Beyond meeting the enhanced demand for data traffic, TSPs also have the incentive to build out networks in underserved regions where there is a large proportion of mobile phone users yet to become data customers.

As the Authority notes in this consultation, there has been a sharp increase in the usage of such communication OTT services, and these, in turn, translate into increased revenue opportunities for TSPs. Moreover, many OTTs already pay TSPs for bandwidth utilized. TSPs are, therefore, already being paid by both users and by OTTs for the bandwidth they use. It is not clear why a regulatory intervention to pay TSPs a third time needs to be introduced.

Analysing all OTTs under a broad umbrella, irrespective of size, might also gloss over the important differences. Several of the largest OTT companies directly invest in infrastructure through investment in the content delivery networks, fibre cable, data centres, and other capital equipment necessary to distribute content over the internet. For smaller upcoming services, on the other hand, any financial requirement to contribute to the financing of network infrastructure beyond the costs of the bandwidth they use would introduce an upfront cost that would likely deter market entry. In effect, there would be a decline in the incentive to invest in creating these OTT services.

If the goal is to incentivise network upgrades, requiring OTTs to pay TSPs a "network upgrade fee" is a short termist, inefficient, and would be detrimental to permissionless innovation that has characterized the internet economy and allowed for its success to

[8] See https://internetassociation.org/wp-content/uploads/2017/05/InternetAssociation-NetNeutrality-Facts.pdf; https://policyintegrity.org/documents/Free_to_Invest.pdf
[9] 3.1-3.3 of TRAI Consultation Paper on Regulation of OTT communication services

date. Such a move would be disproportionately burdensome, and might even deter market entry for SMEs and start-ups as opposed to larger OTT providers. Policy proposals that would deter market entry for new entrants and potentially cause market exit for smaller players, only entrenches already dominant and well-resourced companies.

Q.4 Would interoperability among OTT services and also interoperability of their services with TSPs services promote competition and benefit the users? What measures may be taken, if any, to promote such competition? Please justify your answer with reasons.

We believe that interoperability can be a powerful tool to enhance competition, particularly in the online environment with significant market concentration among a few players who have large network effects. Open and accessible APIs can be a powerful tool for efficient, rapid scaling market entry, when, say, a new app or service developer can reach users through existing APIs offered by platforms that have already achieved significant economies of scale. In general, we would urge the Authority to encourage policies promoting interoperability in the telecommunications space and to play a proactive role in highlighting the role of open APIs in providing access to essential data and functionalities.

However, we would caution against any blanket regulatory mandate that would *force* interoperability as we believe it could have adverse effects on innovation, privacy, and security. In particular, forcing interoperability of SMS services (largely unencrypted) with OTT services is likely to weaken and dismantle the strong, privacy-enhancing encryption offered by many OTT services. Mozilla believes that strong and reliable encryption is a key tool in improving user security, and we should not be encouraging policies that regress away from this ideal. Any design mandates on all OTT providers, especially ensuring interoperability with traditional TSP services, imposes a non-trivial burden on these entities. Forcing interoperability with existing, decades old telecom standards will likely inhibit the development of innovative functions and features.

Q. 5. Are there issues related to lawful interception of OTT communication that are required to be resolved in the interest of national security or any other safeguards that need to be instituted? Should the responsibilities of OTT service providers and TSPs be separated? Please provide suggestions with justifications.

As we have observed in response to TRAI's recommendations on data protection, existing regulations on TSPs vis-a-vis lawful interception, monitoring, and encryption are in dire need of reform. This is particularly true in light of the Supreme Court's clear diktat in the *Puttaswamy v Union of India* decision, which lays down specific limitations on state intrusions into the fundamental right to privacy. Many of these worrying stipulations are also mirrored in the Information Technology Act (and corresponding rules) and apply more broadly to all OTT providers as well. Overall, there appears to be a broad overlap in the the requirements on OTTs and TSPs, as is evident from a comparison of the Unified License applicable to TSPs and the Information Technology Act, 2000 (IT Act) and corresponding rules. Therefore, instead of focussing on ensuring further regulatory parity to the extent it doesn't already exist, we urge TRAI to take this critical opportunity to reform these regressive provisions across the board. As illustrative examples:

- **Power to order setting up of interception and monitoring facilities** *(UL Condition 39.12 and Rules Section 69 of the Information Technology Act, 2000)* : The license condition requires that entities, “in the interests of security”, set up “suitable monitoring equipment” as per the requirements of security agencies – “as and when” they may require them. The interception rules under Section 69 of the IT act allows broad permissions for directives to "provide all facilities, cooperation and assistance for interception or monitoring or decryption"[10]

  We believe that compelling companies to modify their infrastructure based on government requests denies them the ability to provide secure products and services to their customers, undermining trust as well as the success of Indian businesses in the global marketplace. For Mozilla, our products are open source and free software. Not only is our software available for download free of charge, but also any user has access to the source code, and may freely modify and redistribute it. This means that changes to our software are fundamentally public. Were we compelled to create a version of Firefox that was modified to permit surreptitious intrusion subject to a government order, say under Section 69, such modifications could and would be discovered by the Mozilla community.

  These broadly worded obligations require urgent re-examination and are unlikely to fulfil the standard of proportionality laid down by the Supreme Court of India in *Puttaswamy* v *Union of India*.

[10] Rule 13, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

- **Prohibition on bulk encryption and power to issue decryption orders** (UL Condition 37.1 and Rules under Section 69 of the IT Act): The current license term bluntly restricts any “bulk encryption” by licensees. On the other hand, Rule 5 of the interception rules under the IT Act allows for the government to issue "decryption directions" for the decryption of any stored information "involving a computer resource".

We believe any such requirements to undermine encryption pose a severe threat to trust online and to the effectiveness of the internet as an engine for our economy and society. Security and privacy are essential parts of the user experience. We and other browser makers are pushing for a fully encrypted Web in order to protect users everywhere. The use of encryption is growing daily, protecting more and more communications from interference and interception. The overwhelming majority of online traffic belongs to law-abiding citizens, and has no connection to any legitimate governmental purposes. We believe that all internet users have an expectation of privacy in the network exchange of their communications, and companies and technologists continue to support this expectation through policy and through technology. As several leading cybersecurity experts articulated in a recent technical report, proposals to require a government backdoor into digital communications “are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security.”[11]

The existing provisions in the IT Act and the UL make it far too easy to order decryption en masse, or (as in the case of the UL) prohibit encryption measures entirely. This seems disproportionate to any legitimate law enforcement demands sought to be achieved, and stand on shaky constitutional footing following the judgment in *Puttaswamy v Union of India*.

While TRAI has acknowledged in its most recent data protection recommendations that encryption is critical to a safe and secure web, we urge the Authority to make a clear recommendation for the repeal of this regressive condition.

Q. 6. Should there be provisions for emergency services to be made accessible via OTT platforms at par with the requirements prescribed for telecom service providers? Please provide suggestions with justification.

[11] http://dspace.mit.edu/handle/1721.1/97690

In principle, we see the benefits of having emergency calls be accessible on all widely used communications channels, and welcome attention to this important issue. However, we acknowledge that such a move may be accompanied by costs to implement changes to both the emergency response infrastructure of the government (given that OTTs are not currently interconnected to the public switched network) as well as for OTTs (including start-ups and SMEs entering this space). As such, the relative benefit provided by allowing for this facility on OTT communication services should be weighed against these costs before imposing any mandates.

We would support the view taken by TRAI in its previous Consultation on the Regulatory Framework for Internet Telephony[12], where the Authority concluded: *"In view of the above, the Authority recommends that the access service providers providing Internet Telephony service may be encouraged to facilitate access to emergency number calls using location services; however they may not be mandated to provide such services at present."*

Q. 7. Is there an issue of non-level playing field between OTT providers and TSPs providing same or similar services? In case the answer is yes, should any regulatory or licensing norms be made applicable to OTT service providers to make it a level playing field? List all such regulation(s) and license(s), with justifications.

As we describe through this submission, we do not agree with the premise of creating regulatory parity between OTTs and TSPs. Where we think that existing regulations could do with reform, such as on issues of data protection or interoperability, we have indicated as such above.

Q. 8. In case, any regulation or licensing condition is suggested to made applicable to OTT service providers in response to Q.7 then whether such regulations or licensing conditions are required to be reviewed or redefined in context of OTT services or these may be applicable in the present form itself? If review or redefinition is suggested then propose or suggest the changes needed with justifications.

Same as above.

[12] https://www.trai.gov.in/notifications/press-release/trai-releases-recommendations-regulatory-framework-internet-telephony