mozilla

June 29, 2016

TO:
RS Sharma
Chairman, Telecom Regulatory Authority of India

CC:
Shri A. Robert J. Ravi
Advisor (QoS), Telecom Regulatory Authority of India

Dear Sirs,

Re: Comments by the Mozilla Corporation on the Telecom Regulatory Authority of India's Pre-Consultation Paper on Net Neutrality

Thank you for the opportunity to provide comment and input on this Pre-Consultation paper on Net Neutrality, a topic of great importance to protecting the Internet and users in India and around the world. We welcome this discussion of the appropriate regulatory framework for protecting net neutrality, and believe that action is needed in order to ensure the Internet's continued openness.

The Mozilla Corporation produces the Firefox web browser and the Firefox OS ecosystem for connected devices, together adopted by half a billion individual Internet users around the world. Mozilla is also a foundation that educates and empowers Internet users to be the Web's makers, not just its consumers. Finally, Mozilla is a global community of technologists, thinkers, and builders, including thousands of contributors and developers in India, who work together to keep the Internet alive and accessible.

As our Executive Chairwoman Mitchell Baker noted in a May 5th, 2015 letter to Prime Minister Modi: "Net neutrality is critical to maintaining the continued success of the open Internet as an engine for innovation, opportunity, and learning. We stand firm in the belief that all users should be able to experience the full diversity of the Web. For this to be possible, Internet Service Providers must treat all content transmitted over the Internet equally..."[1]

As the TRAI rightfully notes in this pre-consultation paper, "Adherence to this principle of net neutrality is arguably necessary for maintaining the open and non-discriminatory character of the Internet, features that are responsible for the phenomenal growth of the Internet in the past decades."

While we value the protections enshrined in TRAI's Differential Pricing Regulation, we believe further action is needed to protect the core principles of net neutrality. We remain at your disposal for any further information or clarification on any of these points. We look forward to working with TRAI throughout this critical process.

[1] https://ffp4g1ylyit3jdyti1hqcvtb-wpengine.netdna-ssl.com/netpolicy/files/2015/05/Letter-from-Mozilla-

1) What should be regarded as the core principles of net neutrality in the Indian context? What are the key issues that are required to be considered so that the principles of net neutrality are ensured?

Definition and core principles of net neutrality
The open Internet relies on many technological and legal assumptions for its continued vitality. One of those assumptions is net neutrality. Net neutrality is grounded in three principles:

1. *The end-to-end principle*: All points in the network should be able to connect to all other points in the network;
2. *The best efforts principle*: TSPs should deliver all Internet traffic from point to point as expeditiously as possible; and
3. *The innovation without permission principle*: Everyone and anyone should be able to innovate on the Internet without seeking permission from anyone, any entity, or other gatekeeper.

In practice, net neutrality means that TSPs should treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, or means of communication. We strongly concur with the recommendation that all TSPs should be bound to follow and uphold net neutrality.

Taken together, this definition and these principles are critical to ensuring the continued openness of the Internet and ensuring the Internet exists as a level playing field that enables and supports innovation, competition, and opportunity. Indeed, the laudable goals of the Government of India's Digital India initiative will not be possible without these protections for the open Internet. We strongly urge TRAI and the Government of India to include both this technical definition and these principles in any forthcoming regulation on net neutrality.

Discrimination on the basis of features
Throttling and blocking of specific applications or services are the most commonly cited violations of net neutrality. But the net neutrality imperative to treat all types of Internet traffic equally must also be understood to prohibit discrimination on the basis of the *features* of content, applications, and services. The following are some concrete examples of how this distinction could be problematic in the case interpretation permits discrimination based on "features" or "types" (determined by features) of traffic:

- *Encrypted traffic:* Some actors may seek to discriminate against encrypted traffic by treating encryption as a unique "type" or "feature" of traffic, even if there are otherwise no fundamental technical distinctions. This is problematic for Internet businesses and citizens, as such discrimination could prompt end-users to rely more on unencrypted communications, creating perverse incentives to avoid privacy enhancing technologies. Discrimination against encrypted content is also concerning from a competition perspective, as it could be used to enable the creation of preferred classes, artificially separating their traffic from that of their competitors in order to work around the rules. End-users should benefit from both speed and security; the two should not be pitted against one another.

- *Anticompetitive practices:* Network operators may contend that their specific offering(s) or the offering(s) of their partners have unique features which justify prioritised treatment over their competitors. For instance, if a provider has entertainment content offerings that are locally cached, the provider may prioritize traffic that's locally cached over other traffic, and claim that it is doing so for network management purposes, while refusing to allow other service providers to

cache traffic locally. In this case, although the provider is not facially discriminating against or in favor of any specific traffic or categories of traffic, the result is nevertheless intentionally anti-competitive and should not be permitted.

- *Discrimination based on provider:* Conversely, a network operator may consider the traffic of a provider or set of related providers to constitute a specific category unto itself, or to possess unique features, which allegedly justify downgraded treatment. For example, a network operator may allege that YouTube and Skype are too high-bandwidth and thus should be throttled, while the operator's own video streaming and conferencing solutions are less used and thus less bandwidth consuming and are not throttled. Again, an act that appears on its face to be motivated by technical means is in fact motivated by anti-competitive ends.

- *Future innovation:* Another potential challenge is that the technical characteristics of a "type" of application today may not be the same in the future, as the technologies evolve and add new functionality. So even if treatment for a "type" seems reasonable on its face today, may tomorrow produce harmful outcomes for users and the open Internet.

Violations of net neutrality which should be prohibited
As TRAI notes in Paragraphs 19-20 of this Pre-Consultation Paper: "the Unified License that set out the scope of Internet services specifically require TSPs to ensure that subscribers have unrestricted access to all content available on Internet, subject only to lawful restrictions. Any action by TSPs to intentionally and arbitrarily apply restrictions on users' access to the open and neutral Internet would impede user choice."

TRAI has already rightfully recognized some of the most flagrant ways that TSPs may unreasonably interfere with Internet traffic:

- Blocking of applications, websites or any other content on the Internet;
- Slowing or "throttling" Internet speeds;
- Preferential treatment of applications, websites or any other content on the Internet;
- Discriminatory tariff for data services based on the applications, websites or other content being accessed by the user (which has already been prohibited by the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016); and
- Inspection of the contents of data packets, except to meet lawful requirements or to maintain the security of the network.

Explicitly prohibiting these practices in any forthcoming regulation on net neutrality will make clear that they do not constitute lawful or reasonable restrictions, and is critical to ensuring the protection of the Internet's openness.

2) What are the reasonable traffic management practices that may need to be followed by TSPs while providing Internet access services and in what manner could these be misused? Are there any other current or potential practices in India that may give rise to concerns about net neutrality?

Reasonable traffic management practices
Traffic management practices should only be considered reasonable when they are utilized for the purposes of technical maintenance of the network (e.g., to block spam, malware, and attacks on the network), or to mitigate the effects of network congestion under suitable circumstances.

Generally speaking, network congestion can occur due to two conditions:
1) As a result of unpredictable, irregular, and/or temporary network overload; or

2) As the result of a TSP's failure to develop sufficient capacity to handle the network load (which would lead to frequent and sustained windows of network congestion).

In this sense, congestion occurs under exceptional circumstances of unpredictable situations, and reasonable traffic management should be permitted to address these situations. However, the concept of reasonable traffic management should and must be strictly limited to circumstances of unpredictable load at irregular times (condition 1), and must not be used as a cover for systemic underinvestment in network capacity (condition 2).

The Department of Telecommunications recommendations on traffic management as summarized in Paragraph 24(b) of this Pre-Consultation Paper provide additional guidance that the TRAI and the Government of India would be well served to include in any forthcoming regulation on net neutrality:

"(b) Legitimate traffic management practices may be allowed subject to the core principles. The general criteria against which these practices can be tested may *inter alia* include:

- Adequate disclosure to users about traffic management policies and tools to allow them to make informed choices.
- Application-agnostic controls may be used but application-specific control within the "Internet traffic" class may not be permitted.
- Practices like deep packet inspection should not be used for unlawful access to the type and contents of an application in an IP packet.
- Improper (paid or otherwise) prioritisation may not be permitted."

Specialised services

While not specifically addressed in this Pre-Consultation Paper, we encourage TRAI and the Government of India to consider the topic and appropriate limitations on specialised services in any forthcoming regulation on net neutrality.

Specialised services should be understood as electronic communication services which are distinct from Internet access services and provide a specified level of quality of service generally optimized for specific content, applications, services, or some combination thereof. Such optimisation is necessary in order to meet the specific requirements for the specific level of quality. Specialised services are notable in the current context in that they are sometimes justified by TSPs as a mechanism for reducing network congestion; we believe the use of specialized services in this manner should be subject to strict oversight and limitations.

Technically speaking, specialised services can be engineered in (at least) three distinct ways. First, they could be provisioned over distinct physical infrastructure, as separate wires and other hardware. Second, they could be provisioned as channels within the open Internet access service, using bandwidth allocated for the Internet access service but on a different priority level to achieve the desired quality threshold. Finally, they could be provisioned as channels that use the same physical infrastructure but a separate logical capacity, virtually walled off from the open Internet service.

The first type of service is both physically and logically distinct from Internet Access Services and thus the least problematic to assess in terms of its potential conflicts with the requirement to treat traffic in a non-discriminatory manner. Our answer will will thus set this variety aside from further consideration, and will address the second and third types in greater detail.

Both the second and third types may be desirable for content providers because they allow some traffic to "cut through" congestion or other delays associated with the open Internet service. The primary technical

improvement is likely to be reduced latency and jitter for the content delivered by the specialized service, "smoothing" out the transmission pathway regardless of "noise" and traffic load associated with the open Internet service; in some circumstances, bandwidth might be improved as well.

As compared to the second variety, the third, logical separation over shared physical infrastructure, offers the same benefits for the ancillary services with fewer potential harms to competition as compared to shared logical channeling. Sharing both the physical and logical infrastructure (the second variety) is functionally comparable to paid prioritisation arrangements over the open Internet access service, something recognised widely as harmful to competition, innovation, and user choice. In this variety, in the same way as paid prioritisation, giving a benefit to one causes practical harm to others (in that the capacity they could use is less than it would be if the specialised service were not actively in use), as well as challenging the user's expected bandwidth for their open Internet access service (as some of that capacity is cannibalised by the specialised service).

In contrast, logical separation (the third variety) isolates and protects the capacity available to the open Internet access service. Use of the specialised service does not create congestion nor performance benefits for uses of other content, applications, and services on the open Internet. Although the total bandwidth available to the end user for open Internet connectivity is less, suitable disclosures can be made up front, and users will be better empowered to choose whether or not they wish to subscribe to specialised services and thereby limit their open Internet usage.

It's highly unclear whether specialised services are necessary. Often, the contextual problems used to justify their "need" could just as easily be remedied through infrastructure investment, with far more significant benefits for the ecosystem as a whole. The benefits are also highly dependent on the nature of the implementation, and the source of delays associated with the open Internet connection.

We respectfully suggest that TRAI and the Government of India would be served well by establishing principles and a regulatory framework for specialised services in any forthcoming net neutrality regulation in order to best protect the Indian digital economy, Indian users, and the open Internet in the face of future changes to business models and practices. Regulatory vigilance and guidance will be needed to address new innovations and novel, more subtle threats to net neutrality in this fast-changing sector.

Closed networks

In the Regulation on Data Services, TRAI noted an exemption to the Regulation's restrictions on differential pricing for "closed networks":

"Differential tariffs being offered for data transmitted over closed electronic communications networks, such as intranets are not prohibited by these regulations. Though the prohibition on discriminatory pricing of data services does not apply to such networks, which are not accessing the internet, if such a closed network is used for the purpose of evading these regulations, the prohibition will nonetheless apply."

While this is a strong protection, especially when combined with the regulatory principle that "what is done directly cannot also be not done indirectly" (Paragraph 30), there has been some concern that this provision on closed networks could still be exploited to offer a communications service that violates the prohibition on differential pricing as well as any forthcoming regulation on net neutrality. To that end, we respectfully suggest that TRAI might be well served to articulate some additional regulatory guidance to further curtail evasions of these core protections. Specifically, we suggest that any electronic communications service that is available to the public should be obligated to abide by: 1) the prohibition on differential pricing in the Data Services Regulation, 2) any forthcoming regulation on net neutrality, and 3) the Robust Internet Connectivity Principle (for more detail, please see our answer to question 3

below). By focusing on whether a service is available to the public, such a provision would effectively exempt a service like a corporate intranet but would apply to a B2B or specialised service that seeks to masquerade as a closed network in order to violate net neutrality. However, TRAI may wish to exempt services like WiFi on planes from these regulations; this can be effectively accomplished by specifying that this exemption only applies to electronic communications offerings that are not ancillary to a communications service.

3) What should be India's policy and/or regulatory approach in dealing with issues relating to net neutrality? Please comment with justifications.

Concurrent to the exponential increase in the number of connected users and devices, there has also been increasing innovation in new solutions for connecting people as well as new services being offered over the Internet. This is more true in India than perhaps anywhere else. While TRAI's Regulation on Differential Pricing earlier this year has notably already provided a measure of clarity on what practices are too discriminatory to be permitted, TRAI's recent Consultation Paper on Free Data is indicative that we should expect further development and experimentation with additional models for connected the unconnected. While the Differential Pricing Regulation dealt with a specific set of business models and practices, a broader net neutrality regulation that establishes clear rules of the road will be both helpful and instructive.

In this fast growing and fast changing environment, it is imperative that India adopt a policy and regulatory approach that provides both sufficient legal clarity on what practices are permissible and is sufficiently forward looking to address future innovations. To this end, based on our extensive experience working on net neutrality issues in five continents, we believe that a policy/regulatory approach that combines a series of bright line rules and general principles will best serve India's interests and digital economy.

We suggest that the first four types of activities identified in Paragraph 17 of this Pre-Consultation Paper ought all be prohibited under bright line rules. Each of these prohibitions should be subject to an exception for reasonable network management practices, as described above. With regard to the inspection of content of data packets described in Paragraph 17, we note that reasonable network management as employed today, in practice, utilizes networking equipment that looks beyond packet header information in the ordinary course of its operation. We suggest that this category of activities would be better served by coverage under a broader principle, rather than a bright line rule.

As a supplement to these bright line rules and TRAI's existing regulatory principles[2], we encourage the formal adoption of four guiding principles to allow for a more flexible framework, allowing the fundamental bright line rules to be suitably interpreted with the future evolution of technologies and market practices:

[2] As articulated in TRAI's previous Consultation Paper on Differential Pricing for Data Services, Paragraph 9: "Two key principles of tariff regulation emerge in this regard – first, the principle of non-discrimination and second, transparency. Regulation must strive to seek a balance between ensuring wider access to the internet, and the manner in which such wider access is provided does not violate these principles. Offers involving free or reduced rates have to be studied in this context, and within the broader tariff regulatory regime. The Authority monitors the tariff for various services offered in the country through the reporting mechanism put in place. While scrutinizing the tariff proposals, TRAI checks Their consistency with various regulatory principles/guidelines, which include the following: Non-discriminatory, transparency, not anti-competitive, non-predatory, non-ambiguous, and not misleading."

1. Net neutrality requires conscious and continuous attention to preserving **innovation without permission**. If new services, terms, or conditions are allowed to impact creation and invention, then the purpose of the framework will have been undermined.
2. Net neutrality requires **meaningful user choice**. Users must be free to choose content, applications, and services without any artificial weightings placed on the scale, or gates or obstacles placed in front of non-preferred options.
3. Net neutrality requires **robust connectivity and technical performance** that scales along with user needs and expectations. Should TSPs be allowed to weaken open Internet connections in favor of closed systems, the network as a whole would suffer.
4. Net neutrality requires **transparency and meaningful user control** regarding the collection of data by TSPs. Net neutrality cannot achieve its potential if users do not trust their Internet connection and the privacy of their use of it.

While TRAI should continue to make use of its powers to review new tariff offerings, the aforementioned approach combining bright line rules and general principles is far preferable to relying solely on case-by-case determinations. As TRAI noted in its Regulation on Differential Pricing in Data Services (Paragraph 27):

> "A case-by-case regime will fail to provide much-needed certainty to industry participants. In the absence of a clear rule setting out the permissible and impermissible business practices, service providers may refrain from deploying network technology. This would be due to the fear that their conduct may subsequently be construed as being discriminatory as per the case-by-case analysis. Second, it will create high costs of regulation on account of the time and resources that will be required for investigating each case. It will also lead to further uncertainty as service providers undergoing the investigation would logically try to differentiate their case from earlier precedents. Third, there is also the concern that this approach provides a relative advantage to well-financed actors and will tilt the playing field against those who do not have the resources to pursue regulatory or legal actions. This may include end users, low-cost innovators, start-ups, non-profit organizations, etc. The Authority believes concerns are significant." [3]

In regards to how any forthcoming regulation on net neutrality should be enforced, we respectfully concur with the recommendations of the Department of Telecommunications as articulated in Paragraph 24(g) of this Pre-Consultation Paper, and believe that these recommendations if enacted would serve as a strong foundation for an enforcement regime.

4) What precautions must be taken with respect to the activities of TSPs and content providers to ensure that national security interests are preserved? Please comment with justification.

In previous consultations undertaken by TRAI and DOT there has been some speculation about how best to ensure that Over-The-Top (OTT) providers are sufficiently doing their part to protect national security. Specifically, it was envisaged in previous consultations that OTT providers should be made subject to the same licensure requirements as TSPs. We reiterate here the concerns we submitted in response to the DOT's consultation in August of last year:

> "We wish to express concern around proposals that would require a license to operate an online service. As the Committee's report discusses, a central pillar of net neutrality and a major contributing force to the Internet's success has been the concept of "innovation without permission." This concept allowing anyone to develop a new technology, to write

[3] http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf

code and test in the public, and to control the code running on their machines is the lifeblood of the open Internet and the ethos of open source."

As our Executive Chair Mitchell Baker wrote in a letter to Prime Minister Modi in regards to a similar proposal by the Telecom Regulatory Authority of India, any mandatory 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." To this end, we respectfully caution you from proposing any licensing regimes on Internet services or Over-The-Top (OTT) applications, as doing so would only serve to create legal uncertainty, chill innovation, and hurt the promise of Digital India.

Indeed, as TRAI notes in summarizing the DOT's findings in Paragraph 24(f) of this Pre-Consultation Paper: "For OTT application services, there is no case for prescribing regulatory oversight similar to conventional communication services."

While all tech companies have certain responsibilities in regards to national security, this typically comes in the form of trying to make our products and our users as secure as possible. Indeed, any effort to undermine the security of users or Internet services or infrastructure would likely prove atavistic to the broader goals of enhancing national security. Moreover, given the rapidly changing nature of security threats, such matters are best addressed outside of the regulatory context.

5) What precautions must be taken with respect to the activities of TSPs and content providers to maintain customer privacy? Please comment with justification.

We share TRAI's concern that protecting the privacy of customers of Internet and telecommunications services is of the utmost importance. Although the provisioning and management of these services, in particular traffic management practices, may very well raise privacy concerns, this is a complicated and nuanced issue space that is generally best addressed in the context of a separate regulatory or legislative process on privacy and data protection. Including general principles on the importance of protecting user privacy in the context of any forthcoming regulation on net neutrality is welcome, but we respectfully suggest that TRAI, the Government of India, Indian businesses, and Indian users would be best served by developing a comprehensive framework on privacy and data protection, and that developing such a framework should become a national policy priority.

6) What further issues should be considered for a comprehensive policy framework for defining the relationship between TSPs and OTT content providers?

In brief, we commend to the attention of TRAI and the Government of India the complex issues that can arise with interconnection and peering of network traffic, beyond the "last-mile" portion of the network that faces users. Certain practices by network operators at this level of the network infrastructure can have measurable effect on the performance of end users' connections, and can thus undermine the principles and objectives of net neutrality. We encourage TRAI and the Government of India to bear the principles we propose in mind in any future engagements in this technical context, and we suggest that you consider reviewing a reference paper developed by a neutral group of technical experts on the many aspects of this issue.[4]

Respectfully submitted by:

[4] http://bitag.org/report-interconnection-traffic-exchange.php

Denelle Dixon-Thayer
Chief Business and Legal Officer, Mozilla Corporation

Chris Riley
Head of Public Policy, Mozilla Corporation

Jochai Ben-Avie
Senior Global Policy Manager, Mozilla Corporation