mozilla

March 15, 2017

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 Net Neutrality

Dear Sirs,

Thank you for this opportunity to provide comment and input on this Consultation Paper on Net Neutrality. We commend TRAI for the thorough and thoughtful treatment of this topic of great importance to protecting the internet as well as users in India and around the world. We welcome this discussion of the appropriate regulatory framework for protecting net neutrality, and believe that regulatory action is needed in order to ensure the internet's continued openness.

The Mozilla Corporation produces the Firefox web browser 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 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]

To this end, following this consultation process, we respectfully recommend TRAI enact strong net neutrality rules, which are critical to protecting users, competition, innovation, and the full potential of the internet.

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

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

We respond to the questions of the Consultation Paper in detail below, and we remain at your disposal for any further information or clarification of these points.

Q.1 What could be the principles for ensuring nondiscriminatory access to content on the Internet, in the Indian context? [See Chapter 4]

Definitions and principles
As we wrote in our submission to TRAI's pre-consultation on net neutrality:[2]

> "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 should be defined as a requirement that TSPs treat all data on the internet without discrimination, restriction, or interference no matter the sender, receiver, content, website, platform, application, feature, attached equipment, or means of communication, or any types thereof. A strong requirement against discrimination, restriction, and interference is critical in the Indian context.

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 to include both this technical definition and these principles in any forthcoming regulation on net neutrality.

As we elaborate below, a limited exception to the requirements of net neutrality must be allowed to enable TSPs to reasonably manage their networks to mitigate congestion and attacks on the network. It is critical that traffic management practices be considered reasonable only if they are exceptional, temporary, and not arbitrary or discriminatory in their effects or application.

Violations of net neutrality which should be prohibited
In addition, we recommend that certain practices be explicitly prohibited with bright line rules in any net neutrality regulation. As we stated in our response to TRAI's Pre-Consultation Paper on Net Neutrality:

> "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:

[2] https://blog.mozilla.org/netpolicy/files/2016/06/TRAIPre-ConsultationOnNetNeutralitySubmission-FINAL.pdf

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

- 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 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."

Discrimination on the basis of features

We're pleased to see that TRAI specifically recognized the threat to net neutrality -- and by extension to users, competition, and innovation -- posed by discrimination on the basis of features. While throttling and blocking of specific applications or services are the most commonly cited violations of net neutrality, TRAI must consider and address in this regulation more pernicious means to undermine net neutrality.

As we noted in our submission to TRAI's Pre-Consultation Paper on Net Neutrality:

"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, 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

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

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."

Q.2 How should "Internet traffic" and providers of "Internet services" be understood in the NN context? [See Chapter 3]

(a) Should certain types of specialised services, enterprise solutions, Internet of Things, etc be excluded from its scope? How should such terms be defined?

"Internet" and "Service" are already defined in the Unified License granted to TSPs, and we see no reason to deviate from those definitions.

Two criteria are paramount when considering whether a given service is an internet service or not:

1. Whether the service is generally available to the public; and
2. Whether the service can reach all or substantially all endpoints of the internet.

If both criteria are met, the service should generally be considered an internet service and therefore regulated by net neutrality. Furthermore, if a service competes with an internet service and offers some direct access to internet endpoints then it should be considered an internet service, and therefore regulated by net neutrality. In practice, this formulation would appropriately exempt networks like a corporate intranet, a hospital network to share confidential patient records, or a connected refrigerator, but not a service that stands alone in offering connectivity or primarily serves to connect users to the internet.

We further recommend regulatory attention and vigilance to how specialised services are structured. As we noted in our submission to TRAI's Pre-Consultation Paper 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

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

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."

(b) How should services provided by content delivery networks and direct interconnection arrangements be treated? Please provide reasons.

Content delivery networks (CDNs) and direct interconnection are generally good things for the internet and internet users. In contrast to paid prioritization, which is inherently zero-sum, direct interconnection, CDNs, and peering are generally additive to network capacity and efficiency. In addition to often helping to deliver internet traffic more quickly and stably, interconnection, CDNs, and peering can also have the effect of making more bandwidth available over other routes. In general, CDNs and direct interconnection arrangements are not generally available to the public nor do they allow access to all or substantially all end points on the internet, and as such should be regulated outside the scope of net neutrality agreements.

However, to anticipate and prevent any negative effects on users, competition, and innovation from either CDNs and direct interconnection arrangements or specialised services, we would recommend TRAI also include in net neutrality regulation a provision similar to one included in its Data Services Regulation from February 2016, "what is done directly cannot also be not done indirectly" (Paragraph 30).

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

Q.3 In the Indian context, which of the following regulatory approaches would be preferable: [See Chapter 3]

(a) Defining what constitutes reasonable TMPs (the broad approach), or
(b) Identifying a negative list of non reasonable TMPs (the narrow approach). Please provide reasons.

We strongly recommend a "broad approach" to the consideration of traffic management practices. While certain allowances must be made to enable TSPs to appropriately manage their networks from congestion and attacks, these practices are also the easiest and most direct ways to undermine both the spirit and letter of net neutrality regulations. As TRAI rightfully notes in this consultation paper, a narrow approach presents several challenges:

- "Firstly, any narrow approach will be tailored specifically to address the specific challenges that we are aware of today. This may motivate providers to develop other types of business practices that are not explicitly covered in the narrow restrictions although they may have similar harmful effects.
- Secondly, in the example referred to above, lack of commercial motivation could be seen as a sufficient guide for reasonableness. On the other hand, it has been argued by various stakeholders that TMP should be narrowly tailored and therefore be temporary, exceptional and nondiscriminatory in their effects or application. Moreover, it is argued that TMP should not be used as a cover for systematic underinvestment in network capacity. A broader approach might be better suited to address these aspects.
- Thirdly, in the absence of an agreement or partnership, a commercial motivation might not always be apparent or explicit. In such a case, making the case that a particular measure is discriminatory would be challenging. On the other hand, the broader approach could use specific principles to assess the discriminatory treatment of traffic (whether it is objective, temporary and proportional) and accordingly arrive at a conclusion on its reasonableness. This might be useful for identifying those TMP that are discriminatory in effect but not evidenced by an explicit commercial agreement or partnership."

As TRAI further notes in this Consultation Paper, the Department of Telecommunications Committee on this matter has also taken a broad approach to understanding the reasonableness of traffic management practices. TRAI would be well served to include in net neutrality regulation the DOT's recommended principles:

- 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."

With regard to the inspection of content of data packets described in the third bullet above, we note that reasonable network management as employed in practice today utilizes networking equipment that looks beyond packet header information in the ordinary course of its operation. However, the legitimate use of deep packet inspection technology for reasonable traffic management should not be used to unnecessarily violate or compromise the privacy of internet users. We further note that India currently lacks a comprehensive privacy and data protection framework, and we reiterate here our strong recommendation that India make enacting such privacy protections a national priority.

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

Q.4 If a broad regulatory approach, as suggested in Q3, is to be followed: [See Chapter 3]

(a) What should be regarded as reasonable TMPs and how should different categories of traffic be objectively defined from a technical point of view for this purpose?

Traffic management practices should only and strictly 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. We strongly recommend that traffic management practices should only be considered reasonable when they are in their effects and application:

- **Temporary –** Limited in duration and accomplished through the least restrictive means necessary to mitigate the threat to the network from congestion or attack;
- **Exceptional** – Limited to unpredictable moments of network congestion or attack; and
- **Non-discriminatory or arbitrary** – Limited to necessary and proportionate responses to threats to the network from congestion or attack based on objective technical need. Any traffic management on the basis of commercial considerations or practices should be considered unreasonable.

The concept of reasonable traffic management should and must be strictly limited to circumstances of unpredictable load and attack at irregular times, and must not be used as a cover for systemic underinvestment in network capacity or to engage in discriminatory practices.

(b) Should application-specific discrimination within a category of traffic be viewed more strictly than discrimination between categories?

Discrimination on the basis of a category of traffic, especially when a category is application-specific presents a slippery slope that frequently lacks a strictly objective technical basis. Consider, for example, the desire of some TSPs to serve video traffic at a slower speed that non-video traffic. While video content, which is particularly bandwidth intensive, may pose greater congestion challenges than other applications, TSPs should address this through reasonable traffic management, rather than permanently and/or arbitrarily discriminating against video content. When experiencing congestion or high network load, it is preferable that TSPs focus their traffic management on all high bandwidth content and/or high traffic users, rather than targeting a specific provider, application, type of application, etc. Similarly, a TSP responding to network congestion should look at categories of traffic on an objectively technical basis (e.g., latency sensitivity), rather than specific applications, services, etc.

Throttling a single content provider, in particular, should be considered impermissibly discriminatory, arbitrary, and unreasonable. As common carriers, it is the obligation of TSPs to deliver all traffic as expeditiously as possible (the "best efforts principle"). Moreover, chronic congestion and long buffering times should be seen as the result of underinvestment by TSPs in network infrastructure, and not as a justification for discriminatory practices.

(c) How should preferential treatment of particular content, activated by a users choice and without any arrangement between a TSP and content provider, be treated?

User-directed prioritization, while often contemplated as a potential category for exemption to net neutrality prohibitions on prioritization and discrimination, has rarely been actually implemented by TSPs in practice. Nevertheless, internet engineers long ago envisioned this potential use case and designed the DiffServ and IntServ protocols. We do not believe that such an exemption is needed in the Indian context. Even when there is no arrangement between a TSP and a content provider, any preferential treatment

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

exception to net neutrality rules like this could still inhibit competition and innovation and could become a dangerous loophole allowing a TSP to undermine net neutrality rules by slipping in a clause into user contracts to convey such a "choice."

If TRAI does, in its considered wisdom, choose to include an exemption for preferential treatment of particular content, activated by user choice, and without any arrangement between a TSP and content provider, then we would respectfully recommend the following requirements on such schemes:

1. The user must make an informed, explicit, and affirmative request for such prioritization;
2. The user's request must be made through real-time signals, without constraints or application-specific decisions by TSPs, specifically by utilizing the DiffServ and IntServ protocols; and
3. The use must be able to revoke or modify their request at any time without penalty.

Q.5 If a narrow approach, as suggested in Q3, is to be followed what should be regarded as non reasonable TMPs? [See Chapter 3]

As noted above, we strongly recommend TRAI take a "broad approach" to the regulation of traffic management practices.

Q.6 Should the following be treated as exceptions to any regulation on TMPs? [See Chapter 3]

(a) Emergency situations and services;
(b) Restrictions on unlawful content;
(c) Maintaining security and integrity of the network;
(d) Services that may be notified in public interest by the Government/ Authority, based on certain criteria; or
(e) Any other services.
Please elaborate.

We believe that the traffic management necessary for the activities contemplated in this question can already be accomplished by the net neutrality framework and traffic management rules outlined above. Granting a special exception for these types of services would create the possibility of substantial loopholes that would undermine net neutrality. Consider that TSPs regularly take action to maintain the security and integrity of the network in ways that do not require any traffic management. Moreover, "security" is a particularly amorphous concept whose definition could be stretched to enable anti-competitive practices. We would thus respectfully recommend TRAI treat these types of services in the same way as traffic management is regulated for all other types of traffic. As we have articulated in our answer to Question 4, this means that traffic management practices must be temporary, exceptional, and not discriminatory or arbitrary in their effects or application.

We also respectfully suggest that TRAI not make any exceptions to net neutrality regulations for government-notified content. As TRAI rightfully notes, "there might also be concerns related to competitive neutrality that would have to be addressed in situations where the notified services operate in a competitive market environment." The Government of India has many such services that operate in a competitive marketplace and many partnerships and other relationships with private sector actors, which a government-notified services loophole could be exploited to confer an unfair competitive advantage to. At a time when the Government of India is seeking to encourage competition and innovation, including through the Made In India initiative, such a loophole would prove dangerous and atavistic.

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

Finally, we would note that TSPs are already required to follow lawful restrictions on content, and therefore there is no need to include a specific provision here.

Q.7 How should the following practices be defined and what are the tests, thresholds and technical tools that can be adopted to detect their deployment: [See Chapter 4]

(a) Blocking;

(b) Throttling (for example, how can it be established that a particular application is being throttled?); and

(c) Preferential treatment (for example, how can it be established that preferential treatment is being provided to a particular application?).

Definitions

Blocking should be defined as any action, restriction, or practice that renders internet traffic, content, an application, a service, or a non-harmful device effectively inaccessible.

Throttling should be defined as any action, restriction, or practice that slows down, alters, restricts, interferes with, degrades, discriminates, or otherwise unreasonably manipulates internet traffic, content, an application, a service, or a non-harmful device.

Prioritization should be defined as any discriminatory or differential treatment of internet traffic, content, an application, a service, or a non-harmful device.

Prioritization, by definition, is engineered by assigning some packets higher priority than others. If a packet routed at line speed through a network encounters no congestion and no active throttling, it is not placed in any queues, and its priority does not matter because there is never an opportunity for a higher priority packet to be placed "ahead" of it. On the other hand, if the packet encounters congestion,[3] it is placed in a queue along with other packets, and priority levels could be used to determine the order in which packets are released from the queue and advanced through the network. As a result, whenever a higher priority packet is bumped up in a queue and effectively given priority, every packet that it passes by is left worse off and suffers degraded performance, in the form of higher latency, increased risk of packet loss, or, in aggregate, lower bandwidth. Prioritization is inherently a zero-sum practice, and inherently creates fast and slow lanes and prevents a level playing field.

In contrast, paid or settlement-free interconnection that involves adding capacity through new ports, or content delivery network services that offer a benefit by reducing the total distance of travel, inherently do not degrade other communications that share the same local network and pass through the same routers. Although interconnection, in particular, may involve harmful practices that cut at the heart of protecting the open Internet, offering a benefit of improved performance through faster interconnection, caching, or content delivery networks represents a very distinct issue from paid prioritization.

Paid prioritization has a distinct degrading effect on other internet service traffic, an effect that creates complex incentives for network operators. For example, offering paid prioritization may encourage artificial scarcity – underinvesting in total network capacity, or delaying investment, to increase the

[3] Congestion, in this context, does not mean only sustained congestion, a network that is overloaded. Even networks with light average utilization encounter sporadic congestion, perhaps for milliseconds at a time, enough to give a benefit to prioritized traffic, even if only in reducing latency and jitter rather than bandwidth. See Barbara van Schewick, "Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like," Stanford L.Rev. (2014), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2459568

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

relative value of priority by making congestion more commonplace. It also represents a visceral deviation from the end-to-end, best efforts history of the internet, meaning that as a practical matter, it's impossible to understand ex ante the full effects and potential negative externalities that could arise. For these reasons, Mozilla strongly recommends that TRAI prohibit prioritization; specifically, we would respectfully suggest that TRAI adopt the recommendation put forward by the DOT Committee in their considerable wisdom that "improper (paid or otherwise) prioritization may not be permitted."

Tools and monitoring

Before discussing the recommended tools and thresholds that would provide evidence of net neutrality violations, it is important to note at the outset that TRAI need not acquire formal evidence of all violations in order for a net neutrality regulation to be effective and in the public interest. A strong regulation has significant merit and practical effect in and of itself in its ability to change and restrict corporate behavior and practices independent of any enforcement action. Indeed, it would be impractical and near impossible to require the regulator to ascertain evidence of all or substantially all violations of a rule in order for there to be regulation on a given issue.

Of course, effective and expeditious enforcement is also critical to realizing the full protections of a net neutrality rule, and monitoring is an essential precursor to enforcement. Given the nature of both how traffic flows across the internet and the means by which net neutrality is violated in practice, it is critical to conduct measurements and monitoring at several points in the network. We would respectfully suggest that TRAI build a monitoring regime that includes:

1. Disclosures by TSPs,
2. Independent testing and sampling, and
3. User experience and reports.

As regards (1) disclosures by companies, we would respectfully suggest that TRAI require regular (at least annual) reporting by TSPs on their traffic management practices and any known violations of net neutrality regulation.

As regards (2) independent testing and sampling, we would commend to TRAI's attention the suite of testing tools offered by the Measurement Lab (M-Lab).[4] M-Lab's tools include tests for speed, latency, jitter, available bandwidth, application-specific blocking, throttling, traffic shaping, and other practices. We note that at this time, we are not aware of any instance of M-Lab in India. We recommend TRAI set up such an instance on each of the country's TSPs and conduct tests at random intervals, which could be accomplished with minimal effort and investment.

As regards (3) user experience and reports, we note that user reports of interference with their internet connection is the harm that net neutrality regulation is most intended to prevent. We note and commend TRAI for already creating an easy and accurate app, the "MySpeed" app, that users can utilize to assess their internet connection and experience. MySpeed, which already boasts more than a million downloads, could be further developed to test for a wider range of net neutrality violations, potentially by including open source code from M-Lab. Moreover, MySpeed could be configured, with appropriate user consent, to send complaints of violations to TRAI, which the regulator could then use as evidence of violations of net neutrality regulation. We would further suggest that a concerted public education and awareness campaign by TRAI could substantially increase the install base of this useful app.

Independent of the MySpeed app, we would also recommend that TRAI create a portal on its website for users; content, application, and service providers; and other entities who may be affected by net neutrality violations to make complaints and provide evidence to TRAI.

[4] https://www.measurementlab.net/

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

Given the many ways that TRAI may acquire evidence of net neutrality violations and the myriad actors who may provide such evidence, it is likely that TRAI will often need to investigate reports before engaging in any enforcement action. To that end, we would respectfully recommend that the TRAI have sufficient investigatory capacity and punitive powers as part of its enforcement regime.

Finally, for more detailed information about how net neutrality is violated as a technical matter including details of thresholds, we would commend for TRAI's attention a recent report from the Broadband Internet Technical Advisory Group (BITAG): "Differentiated Treatment of Internet Traffic."[5]

Q.8 Which of the following models of transparency would be preferred in the Indian context: [See Chapter 5]

(a) Disclosures provided directly by a TSP to its consumers;
(b) Disclosures to the regulator;
(c) Disclosures to the general public; or
(d) A combination of the above.
Please provide reasons. What should be the mode, trigger and frequency to publish such information?

As TRAI rightfully notes, "transparency is one of the key enabling factors toward ensuring adherence to the nondiscrimination principles set forth in any NN framework. Given the significant regulatory capacity required to effectively monitor TSPs' networks, effective disclosure of information pertaining to TMPs and performance characteristics of a network, enables users as well as the regulator to detect violations."

In its discussion of transparency considerations, TRAI is to be commended again for a thorough and thoughtful analysis of the issues. We concur with and strongly recommend that TRAI require reporting from TSPs on the following categories of information:

1. Price information and commercial terms
2. Performance characteristics
3. Traffic management practices
4. Specialised services, and their impact on internet access services

As we note above, net neutrality violations can occur in many different ways and at different points in the network, hence the need for a holistic monitoring as well as transparency regime. We respectfully recommend that TRAI require disclosures to the end user on the aforementioned categories of information at the point of sale. Given that TSPs practices and capacity will likely change over time, additional disclosures of each of these categories of information should be made to the end user on an at least annual basis, and whenever there is a substantial change. These disclosures to the end user should be required to be provided in a clear, comprehensive, and accessible form. Without adequate disclosure to the public, users cannot make informed choices about the services they wish to purchase.

We would also suggest that TRAI require, as the US FCC does, notification to users when their individual use of a network will trigger a TMP, based on their demand prior to a period of congestion and that is likely to have a significant impact on their experience of the internet. Such disclosures are important to helping users to understand any network interference they are experiencing and to modify their behavior accordingly, including potentially by purchasing alternative services.

[5] http://www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

As TRAI notes in this consultation paper, there is more detailed and granular information about each of these categories of information that may be of value to third parties (e.g., content providers and equipment manufacturers). Such disclosure to third parties should be made available on a publicly available website, so as not to create any differential impact and thereby anti-competitive effect in the availability of this information to some actors and not others. TSPs' public disclosures of more detailed technical information help the internet ecosystem as a whole to function more efficiently and effectively, delivering a better experience to the end user.

As we note above, in order for TRAI to carry out its mandate and to appropriately oversee compliance with net neutrality regulation, we also recommend requiring detailed disclosures by TSPs to the regulator on each of these categories of information on an at least annual basis, as well as requiring additional disclosures when there is a substantial change in practices or offerings.

Finally, as TRAI notes in this consultation paper, TRAI requires much of this information to be disclosed already. Furthermore, we believe that TRAI has the power under existing authorities to compel disclosure of additional information on TMPs and specialised services.

Q.9 Please provide comments or suggestions on the Information Disclosure Template at Table 5.1? Should this vary for each category of stakeholders identified above? Please provide reasons for any suggested changes. [See Chapter 5]

We commend TRAI for producing a thoughtful and thorough template for disclosure in this consultation paper. We believe this is a compelling template for disclosures to the public. We would suggest that in the spirit of providing information to users in a clear, comprehensive, and accessible manner, it may also be beneficial to include definitions of each of the terms used in this template. For example, the lay public may not be familiar with phrases like "application specific traffic management."

Above and beyond the intended user-facing disclosures proposed in this consultation paper, additional technical information on traffic management practices could prove invaluable for other service providers seeking to optimize their applications and services. For example, available APIs and precise traffic performance metrics -- the sort of information routinely exchanged with business partners -- would provide valuable to businesses seeking to reach end users over a TSP's network, yet may not make sense for inclusion in a primarily user-facing template. We encourage TRAI to consider the possibility of enhanced disclosure to promote competition and innovation to the fullest degree.

The regulator will likely be interested particularly in specialised services, including information such as whether the specialised service is provisioned over separate physical and/or logical infrastructure, information about how specialised services are affecting internet service offerings, and the details of commercial partners involved in any specialised services.

TRAI may furthermore benefit from additional information provided by TSPs in the enforcement of future policies. For example, as regards traffic management practices, we would recommend TRAI require disclosures on how technically the traffic management is accomplished, what classes if any were used to engage in traffic management, how often TMPs were used, and other, similar information to allow TRAI to understand generally how TMPs are being deployed in evolving network environments.

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

Q.10 What would be the most effective legal/policy instrument for implementing a NN framework in India? [See Chapter 6]

(a) Which body should be responsible for monitoring and supervision?
(b) What actions should such body be empowered to take in case of any detected violation?
(c) If the Authority opts for QoS regulation on this subject, what should be the scope of such regulations?

We strongly recommend that TRAI create a dedicated regulation on net neutrality. As TRAI rightfully notes in this consultation paper, substantial authority for regulating on net neutrality already exists:

- Clause 2.2(i) of the ISP License Agreement provides for access to the Internet and all content available without any access restriction.
- Clause 2.1 of Chapter of the UASL provides that "The subscriber shall have unrestricted access to all the content available on Internet except for such content which is restricted by the Licnesor/designated authority under Law."
- In the explanatory memorandum to the 2016 Data Services Regulation which already bars TSPs from directly or indirectly imposing discriminatory prices for access to data services based on the type of content being accessed, TRAI has emphasized the importance of maintaining the open and non-discriminatory character of the internet. TRAI has said that it was guided by the principles of net neutrality in enacting this regulation.
- Finally, TRAI's regulatory mandate already includes QOS regulation, review of tariff offerings, consumer protection, and ensuring the orderly growth of the telecom sector, all of which would be furthered by strong net neutrality regulation.

We also concur with TRAI's assessments of the risks of not having a strong regulation on net neutrality: "First, there might be a failure or a significant delay in identifying the discriminatory practices being followed by specific service providers. This is because users generally do not have the means or the ability to detect any interference in their access to particular content, particularly, when it is done in the form of selective variation of speeds. Further, at present the Authority has no formal mechanism for seeking such information from consumers, content providers and other members of the public. Second, even when any discriminatory practices do come to light, the Authority may not be in a position to take action against them due to the absence of an empowering legal framework. Third, this may also create some regulatory uncertainty which could affect the business decisions of stakeholders. In light of these factors, the other approach that needs to be considered is the adoption of an ex ante mechanism that restricts any breach of NN principles and lays down the consequences for it."

While much has been made of TRAI's regulatory actions to prohibit discriminatory and differential pricing, urgent action is still needed to prohibit other discriminatory and differential practices, namely a strong net neutrality regulation. We believe TRAI already has the existing mandate and authority to enact such regulation, and we believe TRAI is the appropriate body to monitor and supervise such regulation. As noted above, we believe that in order to fulfill its oversight of net neutrality regulation, TRAI must have dedicated investigative and punitive powers, above and beyond the current practice of financial disincentives.

Q.11 What could be the challenges in monitoring for violations of any NN framework? Please comment on the following or any other suggested mechanisms that may be used for such monitoring: [See Chapter 6]

(a) Disclosures and information from TSPs;
(b) Collection of information from users (complaints, user-experience apps, surveys, questionnaires); or

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

(c) Collection of information from third parties and public domain (research studies, news articles, consumer advocacy reports).

Please see our answer to Question 7 above.

Q.12 Can we consider adopting a collaborative mechanism, with representation from TSPs, content providers, consumer groups and other stakeholders, for managing the operational aspects of any NN framework? [See Chapter 6]

(a) What should be its design and functions?

(b) What role should the Authority play in its functioning?

We believe that TRAI would be assisted in its mandate by working with the Broadband Internet Technical Advisory Group (BITAG) or a similarly structured entity, including setting up such a group in India.

The Broadband Internet Technical Advisory Group (BITAG) is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on broadband network management practices and other related technical issues that can affect users' internet experience, including the impact to and from applications, content and devices that utilize the Internet.

The BITAG's mission includes: (a) educating policymakers on such technical issues; (b) addressing specific technical matters in an effort to minimize related policy disputes; and (c) serving as a sounding board for new ideas and network management practices. Specific TWG functions also may include: (i) identifying "best practices" by broadband providers and other entities; (ii) interpreting and applying "safe harbor" practices; (iii) otherwise providing technical guidance to industry and to the public; and/or (iv) issuing advisory opinions on the technical issues germane to the TWG's mission that may underlie disputes concerning broadband network management practices.

The BITAG Technical Working Group and its individual Committees make decisions through a consensus process, with the corresponding levels of agreement represented on the cover of each report. Each TWG Representative works towards achieving consensus around recommendations their respective organizations support, although even at the highest level of agreement, BITAG consensus does not require that all TWG member organizations agree with each and every sentence of a document. The Chair of each TWG Committee determines if consensus has been reached. In the case there is disagreement within a Committee as to whether there is consensus, BITAG has a voting process with which various levels of agreement may be more formally achieved and indicated. For more information please see the BITAG Technical Working Group Manual, available on the BITAG website at www.bitag.org.

TRAI could help to stand up a BITAG-like entity and engage in regular dialogue with its members, and if TRAI were to do so, we would strongly suggest that TRAI structure this entity as independent from the regulator.

We would also recommend TRAI have regular contacts and dialogue with content providers, nonprofits, consumer advocates, academics, and other parties that might be affected by net neutrality violations. This could be accomplished, for example, with quarterly meetings with TRAI staff as well as a hotline for making complaints.

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •

Q.13 What mechanisms could be deployed so that the NN policy/regulatory framework may be updated on account of evolution of technology and use cases? [See Chapter 6]

While we believe that TRAI should regularly engage with affected stakeholders to understand the evolution of new technologies and use cases, we would strongly recommend against including any formal sunset or review clause. Net neutrality regulations around the world have proven critical both to 1) ensuring the protection of consumers, competition, and the orderly growth of the telecom sector and 2) have been sufficiently future-proof. TRAI should not encourage a rehashing and relitigation of the substantial debate that has taken place in India around net neutrality over the last several years by building in a mandatory review.

Q.14 The quality of Internet experienced by a user may also be impacted by factors such as the type of device, browser, operating system being used. How should these aspects be considered in the NN context? Please explain with reasons. [See Chapter 4]

While quality of a user's experience may differ in minute ways based on the type of device, browser, or operating system being used, net neutrality has never been understood to be a promise to ensure an identical standard of QOS for each user. Rather, net neutrality protects a user's right to freely seek and impart information and to ensure the internet remains an open, level playing field. More directly, net neutrality guided by the principles of non-discrimination, best efforts, end-to-end, and innovation without permission is about constraining the anti-competitive, anti-innovation, and anti-user behaviors of TSPs. While user's can control and choose the devices, browsers, and operating systems that they use and switch relatively easily, they have no such control or choice over TMPs, for example.

We strongly recommend that TRAI keep this regulation focused on net neutrality, and not include ancillary subjects like device neutrality and OTT licensing, which would only serve to complicate, weaken, and distract this regulation.

Respectfully submitted by:

Denelle Dixon
Chief Business and Legal Officer, Mozilla Corporation

Chris Riley
Head of Public Policy, Mozilla Corporation

Jochai Ben-Avie
Senior Global Policy Manager, Mozilla Corporation

331 E. Evelyn Avenue, Mountain View, CA 94041 • tel 650 903 0800 • fax 650 903 0875 •