Counter-comments to Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality

27 February, 2020

By **Torsha Sarkar** and **Kanav Khanna**
Edited by **Elonnai Hickok**

The Centre for Internet and Society, India

Introduction

The Centre for Internet and Society (CIS), is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with diverse abilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, and open access), internet governance, telecommunication reform, digital privacy, and cyber-security.

This submission presents counter-comments by (CIS) in response to the consultation paper floated by the TRAI on the topic of 'Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality'. These counter-comments take stock of the submissions made by commentators on these issue, and also CIS' previous work on areas of net neutrality.

On each issue dealt upon, we summarize the opinions of relevant stakeholders first, and then register our agreement or disagreement with these lines of commentary. This submission is consistent with CIS' commitment to safeguarding general public interest, and the interests and rights of consumers. CIS is thankful to the TRAI for this opportunity to provide feedback to the consultation paper.

About traffic management practices (TMPs)

The issue of traffic management practices (TMP) has continued to be a challenge as the foundations of the internet have continued to develop. While initially deployment of similar hardware, with the availability of excess bandwidth would have sufficed, fast innovation has revealed the limitations of this structure[1]. Such innovation has also changed the nature of content that travels over transmission - from mere text, it has now changed to content that can be only functional if traffic is prioritized[2]. In light of keeping the functionality of the internet afloat therefore, TMPs became necessary.

On the other hand, Dr. Schewick, in her seminal text 'Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like', defines net neutrality as rules that limit "*the ability of Internet service providers to interfere with the applications, content, and services on their networks; they allow users to decide how they want to use the Internet without interference from Internet service providers.*"[3] To that extent, traffic

[1] John Harris Stevenson and Andrew Clement, 'Regulatory Lessons for Internet Traffic Management from Japan, the European Union, and the United States: Toward Equity, Neutrality, and Transparency' <https://www.researchgate.net/profile/John_Stevenson25/publication/46033576_Regulatory_Lessons_for_Internet_Traffic_Management_from_Japan_the_European_Union_and_the_United_States_Toward_Equity_Neutrality_and_Transparency/links/5828d59008ae950ace700d7e/Regulatory-Lessons-for-Internet-Traffic-Management-from-Japan-the-European-Union-and-the-United-States-Toward-Equity-Neutrality-and-Transparency.pdf>
[2] Id.
[3] Barbara van Schewick, 'Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like', Stanford Law Review 67(1) [2015] <shorturl.at/fxGMR>

management practices become paramount, since regulation on this topic would ultimately determine the effectiveness of any net neutrality regime. Our counter-comments below, accordingly keeps the principle of prioritizing user-choice as a primary level concern, while also emphasizing the business aspect of TSPs.

General comments

TMPs in pursuance of legal orders should be clearly demarcated and clear monitoring mechanisms should be enforced.

Summary: Commentators including NASSCOM and Broadband India Forum have argued that any TMPs adopted in pursuance of legal order would be reasonable. However, we clarify this position further, and ask the regulator to clearly define the legal process under which adoption of TMPs would be valid. This view finds concurrence in the views put forward by the Internet Freedom Foundation (IFF).

Additionally, we ask the regulator to institute an enforcement mechanism to ensure that users are able to lodge complaints against TSPs on instances of experiencing web censorship, arising out of the misuse of the legal process.

Our counter-comments: In the original submissions, several stakeholders pointed out that blocking of transmission pursuant to a legal order was an acceptable form of TMP[4]. While we agree in principle, we feel it necessary to emphasize that the regulation must clarify the exact nature of legal order pursuant to which the blocking process could constitute a reasonable TMP. More specifically, the relevant authority must recognize the existing legal framework of blocking in India, which is governed by section 69A and section 79 of the Information Technology (IT) Act, and mandate that *only* blocking pursuant to orders under these sections would comprise as a reasonable form of TMP.[5]

Additionally, the regulatory authority must also recognize that these provisions have certain substantive and procedural fallacies which open them up to misuse, possibly leading to net neutrality violations. In our previous work, we have documented several

[4] 'NASSCOM Response to TRAI Consultation Paper on Traffic Management Practices (TMPs) and Multi-Stakeholder Body (MSB) for Net Neutrality' <https://main.trai.gov.in/sites/default/files/NASSCOM_14022020.pdf>; 'BIF Response to TRAI Consultation Paper on Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality' <https://main.trai.gov.in/sites/default/files/Broadband_India_Forum_14022020.pdf>

[5] Internet Freedom Foundation, 'Comments towards TRAI's Consultation Paper on "Traffic Management Practices (TMPs) and Multistakeholder Body for Net Neutrality"' <https://main.trai.gov.in/sites/default/files/Internet_Freedom_Foundation_14022020.pdf>

problems with section 79 and its allied rules[6] as well as the problems of section 69A and its allied rules[7].

The issue is best illustrated by the series of website blockings that were documented in early 2019. Several users of Reliance Jio, an ISP operating in India, reported that sites like Indian Kanoon, Reddit and Telegram were inaccessible through their connections in different sites. When they tried to access these websites, they were presented with a notice that the websites were blocked on orders from the Department of Telecommunications (DoT). Some of these websites were also blocked inconsistently[8] across other ISPs, including Hathway and Bharti Airtel.[9]

When the owner of Indian Kanoon contacted Reliance Jio, they were told that the website had been blocked on orders of the government and that the order had been rescinded the same evening.[10] However, in response to a Right to Information (RTI) request, the DoT said they had no information about orders relating to the blocking of Indian Kanoon.[11]

These instances are symptomatic of the functioning of an opaque blocking system facilitated by the Indian legal process, leading to violations of net neutrality principles[12]. The authority must take stock of such instances of inconsistent blocking, and ensure that any monitoring mechanism must account for such misuse of the law. To this extent, we ask the regulator to ensure that end-users are provided with a platform to lodge complaints in instances of experiencing such inconsistent blocking and other similar violations of net neutrality.

Deep packet inspection (DPI) cannot be a reasonable form of TMP.

Summary: IFF has argued that deep packet inspection (DPI) and other similar methods of TMP should be explicitly prohibited, since they violate the right to informational privacy of Indian citizens. We agree with this stance, and further enumerate the several privacy risks surrounding DPIs.

---

[6] Gurshabad Grover, Elonnai Hickok et. al, 'Response to the Draft of The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018' <https://cis-india.org/internet-governance/resources/Intermediary%20Liability%20Rules%202018.pdf>;
[7] Torsha Sarkar and Gurshabad Grover ,'Content takedown and users' rights' (12 February 2020, *The Leaflet*) <https://theleaflet.in/content-takedown-and-users-rights/>
[8] We have previously also written about inconsistent techniques used by TSPs to block content in India; *See*: Kushagra Singh, Gurshabad Grover and Varun Bansal, 'How India Censors the Web' <https://arxiv.org/pdf/1912.08590.pdf>
[9] 'Reddit, Telegram among websites blocked in India: Internet groups' (4 April 2019, *Economic Times*) <https://tech.economictimes.indiatimes.com/news/internet/reddit-telegram-among-websites-blocked-in-india-internet-groups/68714815>
[10] 'Reddit, Telegram among websites blocked in India: internet groups' (3 April 2019, *Reuters*) <https://in.reuters.com/article/us-india-internet-idINKCN1RF14D>
[11] IndianKanoon, (17 January 2020, Twitter) <https://twitter.com/indiankanoon/status/1218193372210323456>
[12] IFF, 'What the block! Our net neutrality rules require a monitoring and enforcement structure' <https://internetfreedom.in/what-the-block-our-net-neutrality-rules-require-a-monitoring-and-enforcement-structure/>

Our counter-comments: Deep packet inspection (DPI) allows networks to examine the contents of a data packet, as well as its origin and destination.[13] In reference to traffic management, it allows TSPs to utilize DPI to manage network, QoS and network security. However, this technology has also historically being used for surveillance purposes across governments, including in China[14], Malaysia[15] and Singapore[16].

Additionally, usage of DPI may also suffer from issues of 'mission-creep'[17], whereby once deployed, the technology can also be used for very different purposes, including pattern matching of intercepted content and storage of raw data or conclusions drawn from the data[18] This scope of mission creep is even more problematic as it would be invisible, often without leaving any traces on the user's system, thus rendering them virtually undiscoverable.

Accordingly, we argue that while defining what constitutes as reasonable TMPs, the regulator must explicitly prohibit utilization of DPI and any other similar methods, since that would go on to raise severe privacy concerns and threaten the idea of the internet as an open space[19].

What constitutes a reasonable TMP can be defined in a broad manner.

Summary: TRAI had asked stakeholders to consider what constitutes a reasonable TMP, and as an ancillary point, what framework can be adopted to identify the same. There was some divergence of opinions on this, where some commentators asked for a negative list of TMPs to be prepared, whilst others suggested a broader approach of delineating a list of reasonable TMPs. We agree with the latter stance, and further clarify our position.

Our counter-comments: Koan Advisory Board had stated that TRAI should consider putting out a negative list of TMPs, which lists prohibited practices that must be avoided[20]. On the other hand, Broadband India Forum and IAMAI both argued that identification of

---

[13] Christopher Parsons, ' The Politics of Deep Packet Inspection: What Drives Surveillance by Internet Service Providers' (6 November 2013) <https://www.christopher-parsons.com/the-politics-of-deep-packet-inspection-what-drives-surveillance-by-internet-service-providers/>

[14] 'The Great Firewall of China' (23 January 2006, *Bloomberg Businessweek*) <https://www.bloomberg.com/news/articles/2006-01-22/the-great-firewall-of-china>

[15] Mike Wheatley, ' Malaysia's Web Heavily Censored Before Controversial Elections' (6 May 2013, *SiliconAngle*) <http://siliconangle.com/blog/2013/05/06/malaysias-web-heavily-censored-before-controversial-elections/>

[16] 'Deep packet inspection rears its ugly head' (4 May 2011) <)https://majid.info/blog/telco-snooping/>

[17] Alissa Cooper, 'Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection,' in W. Aspray and P. Doty (Eds.), Privacy in America: Interdisciplinary Perspectives, Plymouth, UK: Scarecrow Press, 2011 at 151

[18] Amber Sinha, 'Deep Packet Inspection: How it Works and its Impact on Privacy' (16 December 2016, *The Centre for Internet and Society*) <https://cis-india.org/internet-governance/blog/deep-packet-inspection-how-it-works-and-its-impact-on-privacy#_ftnref27>

[19] Id.

[20] Koan Advisory Group, 'Response to Consultation Paper on Traffic Management Practices (TMPs) and MultiStakeholder Body for Net Neutrality.' <https://main.trai.gov.in/sites/default/files/Koan_Advisory_Group_14022020.pdf>

reasonable TMPs was a complex issue. Accordingly, the regulator should broadly define what comprises reasonable TMPs, and set out clear guidelines which would determine the reasonableness of any method adopted by the ISPs[21].

In our previous submissions to the TRAI, we had stated that an ideal regulatory approach would be a broader approach, where all relevant stakeholders participate in listing down reasonable TMPs. This approach, while not hindering user-choice, must also ensure that competition among TSPs is effective[22].

We also agree with Dr. Van Schewick's definition of what constitutes a reasonable TMP[23]. According to her, any exception for reasonable network management should require the method to be:

- appropriate and tailored (i.e. only used during times of congestion),
- as application-agnostic as possible (this requirement is key), and
- only apply to the rules against blocking and discrimination.[24]

While specialized services should be exempted from the regulation of TMP, they must also be narrowly drawn.

Summary: There seems to be a divergence of opinion regarding the place of specialized services in TMPs. We agree with commentators who ask for exemption for TMPs, whilst asking for such services to be narrowly drawn, and provide a set list of criteria that must be followed while defining specialized services.

Our counter-comments: Bharti Airtel Limited, in its submission, has argued that specialized services must be kept out of the scope of TMPs, and that TSPs should be allowed to deploy any techniques for the same[25]. This is in direct contrast with views of Mozilla, who argued that specialized services must be subject to "*strict oversight and limitations.*"[26] In between, there are also commentators who said that while specialized services should be exempted, they should also be drawn narrowly to ensure that the TSP does not misuse such exemption[27].

---

[21] BIF Submissions (n 1); IAMAI, 'Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality' <https://main.trai.gov.in/sites/default/files/IAMAI_14022020.pdf>
[22] Pranesh Prakash, Udbhav Tiwari and Pranav Bidare, 'CIS Submission to TRAI Consultation on Net Neutrality' (April 18 2017) <https://cis-india.org/internet-governance/files/cis-trai-submission-on-net-neutrality>
[23] Barbara van Schewick, 'Comments on TRAI's Consultation Paper on Net Neutrality' (March 15 2017) <https://main.trai.gov.in/sites/default/files/Barbara%20van%20Schewick_13_04_2017.pdf>
[24] IFF's submission to the TRAI also supports this definition.
[25] Bharti Airtel, 'Response to Consultation Paper on Traffic Management Practices (TMP) and Multi-Stakeholder Body for Net Neutrality' <https://main.trai.gov.in/sites/default/files/Airtel_14022020.pdf>
[26] Mozilla Corporation, 'Comments of the Mozilla Corporation on the Telecom Regulatory Authority of India's Consultation Paper on Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality.' <https://main.trai.gov.in/sites/default/files/Mozilla_14022020.pdf>
[27] BIF Submissions (n 1), IAMAI submissions (n 16), IFF submissions (n 2)

We agree with the third line of commentary. As IFF points out, the term 'specialized services' is amorphous, and can open up possibilities of misuse by TSPs[28]. Therefore, there is a clear need to define this term to erase ambiguities in regulation. In our previous submissions to TRAI on the topic of net neutrality, we have noted[29] that specialized services should be exempted if they meet the following criteria[30]:

- The service is available to the user only upon request, and not without their active choice and,
- General Internet access (without any form of preferential treatment of any class of traffic) is provided at the same or lesser cost, and,
- The service cannot be reasonably provided with "best efforts" delivery guarantee that is available over the Internet, and hence requires discriminatory treatment, or
- The discriminatory treatment does not unduly harm the provision of the rest of the Internet to other customers.

Enforcement Framework Must Provide for Proactive Monitoring and Disclosure Obligations.

Summary: Several commentators have argued for the enforcement framework to be restricted to complaint or evidence-based approach where monitoring and intervention is mandated only upon the receipt of a complaint/report alleging non-compliance by the internet service provider. While monitoring and investigating complaints alleging breach of net neutrality is an essential component of the enforcement framework, we believe it must also provide for proactive monitoring of traffic management practices.

Our counter-comments: In its submissions, Reliance argued that a reactive regulatory approach would be more suitable than a proactive regulatory approach that is based upon monitoring in response to reporting of a potential breach.[31] Similarly, COAI and Broadband India Forum have also argued for a complaint and probe-based approach i.e. monitoring consumer complaints and conducting a probe in response.[32]

We disagree with this proposition and believe that the framework for enforcing net neutrality must go beyond an evidence-based or complaint and probe-based approach. This is because such a framework will compromise the ability of the regulatory body to ensure compliance with the net neutrality regime. We argue that proactive monitoring of Telecom Service Provider (TSP) practices by the regulatory body is essential in enforcing net neutrality. This must be supplemented with mandatory disclosure of traffic management practices applied by TSPs.

---

[28] IFF submissions (n 2)
[29] Pranesh Prakash, 'Regulatory Perspectives on Net Neutrality' (8 July 2015, *The Centre for Internet and Society*) <http://cis-india.org/internet-governance/blog/regulatory-perspectives-on-net-neutrality>
[30] CIS submissions (n 17)
[31] Reliance Jio, 'Comments on Consultation Paper dated 02.01.2020 on 'Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality' < https://main.trai.gov.in/sites/default/files/RJIL_14022020.pdf>
[32] COAI, 'Response to the TRAI Consultation Paper on 'Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality' <https://main.trai.gov.in/sites/default/files/Broadband_India_Forum_14022020.pdf>

The importance of transparency and disclosure was highlighted in the consultation paper itself. To this extent, Telecom Service Providers (TSP) must publicly disclose information regarding its traffic management practices. Such disclosure must contain information about the TMPs applied by the provider, nature of the TMP, grounds for imposing it and the impact on the quality of the internet access services deployed by the ISP. One way of doing this can be by mandating TSPs to disclose the TMPs adopted in their terms of service (ToS).

A complaint and probe-based approach without such disclosure requirements would inhibit scrutiny of TSP activities and thereby prevent the detection of net neutrality violations. Further, monitoring compliance of TSPs with principles of net neutrality must not merely be performed in response to reporting of an incident and instead be proactive. We agree with other commentators that the approach must be a combination of different methods.[33]

As a part of proactive monitoring, the regulatory body must: first, scrutinise traffic management practices from public disclosure reports issued by the ISPs. Second, the regulatory body must conduct technical traffic management measurements regularly. It may use existing tools in the market to perform such measurements.[34] Alternatively, as suggested by Mozilla, access providers can also be mandated to run measurement tools and publish its results as part of their public disclosure.[35] Third, the regulatory body must also collect data from Internet service providers and users.

Consequently, we disagree with Reliance's suggestion for the industry body to be authorized to collect data on the admission of an incident in breach of the net neutrality principle.[36] We believe that data must be collected from ISPs on a periodical basis independent of any complaints. Thereby, regulators must be formally empowered to collect information. This is consistent with the approach adopted by the UK Regulator OfCom where operators are legally obliged to respond to information requests.[37]

Conclusion

As we have stated before, regulation of TMPs form a crucial part of imparting an effective net neutrality regime. In light of that, we summarize our counter-comments below:

- While several commentators recognize TMPs adopted in pursuance of legal orders as valid and reasonable, we feel it is necessary for the regulator to clarify that only those orders issued under the designated provisions of law, and by designated authority, would count as a valid TMP. Additionally, the authority must also recognize that substantive and procedural loopholes in these legal provisions may

[33] Mozilla submissions (n 21), NASSCOM submissions (n 1), IAMAI submissions (n 16)
[34] IFF submissions (n 2)
[35] Mozilla submissions (n 28)
[36] Reliance Jio submissions (n 26)
[37] OfCom, 'Monitoring compliance with the EU Net Neutrality regulation' <https://www.ofcom.org.uk/__data/assets/pdf_file/0018/103257/net-neutrality.pdf>

open the process up for misuse. Accordingly, they must ensure that internet users have sufficient redressal mechanisms in such instances.

- Deep packet inspection as a TMP is intrusive, and invades upon the privacy of the internet users. Accordingly, the regulator must clearly prohibit the utilization of DPI and any other similar methods as being unreasonable.

- While user-rights should be of primary concern to the regulator, TMP rules must not be framed in a way to hinder competition in the TSP market. Accordingly, what constitutes a reasonable TMP may be defined in a broad, positive list approach, with clear guidelines to determine the reasonableness of any practices adopted by a TSP.

- Specialized services as a class may be exempted from the scope of TMP rules. However, the scope of the term and the exemption must be clearly defined, in line with international best practices.

- Any framework to monitor compliance with TMPs must be proactive and not reactive, and must be supplemented with mandatory compliance and transparency reporting by the TSPs to the regulator about the TMPs they adopt.