Stanford Law School

Barbara van Schewick
Professor of Law and by Courtesy, Electrical Engineering
Helen L. Faculty Scholar
Director, Center for Internet and Society

February 13, 2020

Comments on TRAI Consultation Paper on "Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality"

I welcome the opportunity to comment on the TRAI Consultation Paper on "Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality."

I submit these comments as a professor of law and, by courtesy, electrical engineering at Stanford University whose research focuses on Internet architecture, innovation and regulation. I have a Ph.D. in computer science and a law degree and have worked on net neutrality for the past twenty years. My book "Internet Architecture and Innovation," which was published by MIT Press in 2010, is considered the seminal work on the science, economics and politics of network neutrality. My papers on network neutrality have influenced discussions on network neutrality all over the world.[1] I have testified on matters of Internet architecture, innovation and regulation before the California Legislature, the US Federal Communications Commission, the Canadian Radio-Television and Telecommunications Commission, and BEREC.[2] The FCC's 2010 and 2014 Open Internet Orders relied heavily on my work. My work also informed BEREC's 2016 net neutrality implementation guidelines as well as the 2017 Orders on zero-rating by the Canadian Radio-Television and Telecommunications Commission, and TRAI's 2016 Order on zero-rating. Finally, I served as technical advisor for California's net neutrality law, which took effect in January 2020. I have not been retained or paid by anybody to participate in this proceeding.[3]

My comment draws heavily on my existing writings on net neutrality. The papers most relevant to this consultation are attached to this submission. I would welcome the opportunity to discuss these important issues further.

---

[1] See, e.g., van Schewick (2007); Frischmann & van Schewick (2007); van Schewick (2015b).
[2] See, e.g., van Schewick (2008); van Schewick (2010c); van Schewick (2010b); Federal Communications Commission (2014).
[3] Additional information on my funding is available here: http://cyberlaw.stanford.edu/about/people/barbara-van-schewick.

TRAI should clarify to be considered "proportionate" and, therefore, "reasonable," network management practices have to be as application-agnostic as possible.

The consultation paper suggests that TRAI and/or the Department of Telecommunications (DoT) intend to evaluate traffic management measures currently used by providers of Internet access services in India to ensure they are consistent with net neutrality and meet the requirements for network management practices to be "reasonable."

Before such an evaluation can take place, it is important to clarify the standard that will be used to evaluate traffic management measures. While TRAI already laid out requirements for reasonable traffic management in its 2017 Recommendations on Net Neutrality, these requirements do not currently explicitly state a critical principle that has been a critical part of leading net neutrality regimes around the world – the requirement for traffic management measures to be as application-agnostic as possible.

This principle is already implicitly included in TRAI's requirement that network management has to be proportionate. However, it seems necessary to make this requirement explicit to provide certainty to market participants. Doing so would bring India's net neutrality regime in line with other leading net neutrality regimes, including the FCC's 2010 and 2015 Open Internet Orders, the California net neutrality law (which codifies the net neutrality protections that were in place at the federal level until the FCC voted to eliminate these protections in December 2017) and the net neutrality regimes in Canada and Europe.

Proposed language:

To be considered "proportionate," network management practices has to be primarily used for, and tailored to, achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service, and is as application-agnostic as possible

"Application-agnostic" means not differentiating on the basis of source, destination, Internet content, application, service, or device, or class of Internet content, application, service, or device.

"Class of Internet content, application, service, or device" means Internet content, or a group of Internet applications, services, or devices, sharing a common characteristic, including, but not limited to, sharing the same source or destination, belonging to the same type of content, application, service, or device, using the same application- or transport-layer protocol, or having similar technical characteristics, including, but not limited to, the size, sequencing, or timing of packets, or sensitivity to delay.

This language is drawn from the California net neutrality law SB 822, which took effect in January 2020.[4] The law is widely viewed as a net neutrality model law that will set the standard for other states to follow. SB 822 is the first and, so far, only state-level net neutrality law in the

[4] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB822.

U.S. that truly restores all of net neutrality protections that the FCC adopted in 2015. Prior state-level laws and executive orders just copied the text of the FCC's 2015 net neutrality rules, leaving out critical protections. By contrast, SB822 includes the important protections and clarifications in the full Order which explained the rules and closed known loopholes. The legislators in the state of Maryland and the District of Columbia recently introduced laws that adopted the California net neutrality law for their states.[5]

TRAI's recommendations for net neutrality already implicitly include the requirement for traffic management measures to be as application-agnostic as possible.

TRAI's 2017 Recommendations for Net Neutrality allow providers of Internet access services to engage in reasonable traffic management. As the Recommendations explain, to be considered "reasonable," traffic management measures have to be "proportionate, transient, and transparent."

All of these are critical requirements that ensure that traffic management measures provide as little harm to competition, innovation, and user choice as possible.

However, the Recommendations do not currently require traffic management measures to be as application-agnostic as possible.

Over the past ten years, the "application-agnostic" principle has emerged as a key requirement for reasonable network management under a meaningful net neutrality regime. Whether network management is application-agnostic was a key factor in the evaluations of network management practices under the FCC's 2008 Order against Comcast,[6] the FCC's 2010 Open Internet Order,[7] and the FCC's 2015 Open Internet Order.[8] Similarly, the FCC's Canadian counterpart, the Canadian Radio-Television and Telecommunications Commission (CRTC), has required network management to be as application-agnostic as possible since 2009.[9] This principle plays an important role in the evaluation of network management practices under the European Union's net neutrality regime as well. In all of these instances, the decisions were the result of long, in-depth proceedings that included extensive public comments and hearings.

Both the Canadian and the European net neutrality regime explicitly treat the requirement to be as application-agnostic as possible as a specific kind of proportionality. That makes sense. Traffic management that singles out specific applications or classes of applications creates exactly the kind of harms that net neutrality protections are designed to protect. As a result, it is

[5] Maryland: Commercial Law - Maryland Net Neutrality Act of 2020 (HB0957) mgaleg.maryland.gov/2020RS/bills/hb/hb0957F.pdf; District of Columbia: "Consumer Net Neutrality Protection Act of 2020," www.davidgrosso.org/s/Consumer-Net-Neutrality-Protection-Act-of-2020.pdf.
[6] *FCC 2008 Comcast Order*, paras 47-50.
[7] FCC 2010 Open Internet Order, para 87.
[8] FCC 2015 Open Internet Order, paras. 220 and 221.
[9] Canadian Radio-Television and Telecommunications Commission (2009), para 43 (asking, among other questions, whether a discriminatory network management practice results "in discrimination or preference as little as reasonably possible").

not proportionate to use a measure that harms competition, application innovation, free speech and user choice more if less harmful ways of managing the network are available.

Explicitly codifying the requirement that traffic management should be as application-agnostic as possible is good policy.

Explicitly codifying the well-established principle that network management should be as application-agnostic as possible creates certainty in the market, makes India's net neutrality provisions easier to enforce, and protects Internet users and edge providers from unnecessary harm.

Codifying the principle reduces uncertainty in the market and saves the entity enforcing net neutrality from having to re-litigate a decade of net neutrality precedents to conclude that this requirement should, indeed, be included. In the absence of the clarification that the requirement for traffic management to be proportionate also includes the requirement to be as application-agnostic as possible, ISPs could try to argue that network management practices targeting specific applications or classes of applications are a tailored, and therefore permissible, approach to managing congestion, as long as the discrimination is limited to times of congestion.

Not codifying the principle threatens to expose Internet users in India to avoidable harm. As the experience of the United States, Canada, and the United Kingdom has shown, ISPs have routinely blocked or discriminated against specific applications or types of applications to manage congestion when they were not required to manage their networks in an application-agnostic manner. These practices harmed Internet users and edge providers and created significant collateral damage. For example, ISPs in the UK routinely managed congestion by singling out specific applications or classes of applications. These practices not only prevented users from using the Internet as they want during peak times (when everyone is watching the new Game of Thrones episode) and made it impossible for affected applications to reach their users, but also interfered with applications like online gaming that were inadvertently caught up in discriminatory network management practices not targeted at them. By contrast, Internet users in countries that require ISPs to manage their networks as application-agnostic as possible avoided these problems.

Requiring traffic management to be as application-agnostic as possible is feasible and has worked well in the US and Canada.

In line with these regulatory requirements, large and small ISPs in the US and Canada have successfully managed congestion on fixed networks in an application-agnostic manner for many years.[10] For example, Comcast, the largest provider of broadband Internet access services in the

[10] For the US, see, .e.g., Comcast (2015); Bastian, et al. (2010); Meisner (2008); Frontier (2015); Lightstream (2015); Bretton Woods Telephone Company (2011); Plateau (2013). Canada: Since the CRTC's decision, most of the larger Canadian Internet service providers have changed their practices in response to the regulations regarding network management that the CRTC adopted following its investigation. In January 2012, Rogers remained the only larger Canadian provider that was still engaging in discriminatory network management that had not announced an intention to phase out that policy. Geist (2007); Schmidt (2012).

United States, adopted an application-agnostic congestion management system in response to the FCC's order against Comcast in 2008. According to Comcast, "Comcast's trials and subsequent national deployment indicate that this new congestion management system ensures a quality online experience for all of Comcast's HSI [High Speed Internet] customers."[11] Many wireless ISPs in the United States manage congestion that way, too.[12]

As the experience with the existing net neutrality regimes in the US and Canada has shown, requiring network management to be tailored, appropriate, *and* as application-agnostic as possible gives network providers the tools they need to manage their networks and maintain a quality experience for all Internet users, while protecting the Internet as a level playing field and supporting user choice even during times of congestion or other moments where network management becomes necessary. At the same time, the exception provides a safety valve that allows ISPs to react in more application-specific ways if a network management problem cannot be solved in an application-agnostic way.

For a more detailed description and analysis of the exception for reasonable network management proposed here with citations to the relevant literature, see van Schewick (2015), Network Neutrality and Quality of Service (attached), pp. 137-140, and, for a shorter version, van Schewick (2015), The Case for Meaningful Net Neutrality (attached), pp. 7-11.

Any evaluation of reasonable network management needs to account for the considerable social costs of class-based traffic management.

Internet access providers often argue that they should be allowed to differentiate among classes of traffic for purposes of traffic management, as long as they treat similar applications the same.

Class-based network management has the potential to create enormous social costs, even if it is based on the traffic's objective different technical requirements. Such traffic management practices still allow ISPs to distort competition, stifles innovation, harms users, and hurts providers who encrypt traffic by putting all encrypted traffic in the slow lane.

The following excerpt from one of my recent articles explains why.[13]

"The proposal allows ISPs to engage in class-based discrimination.

The proposal allows class-based discrimination: ISPs can make distinctions between different kinds of traffic and treat them differently to optimize overall transmission quality at any time, not just during times of congestion. The discrimination must be based on the technical requirements of the applications in question. Thus, ISPs could treat different kinds of applications differently if they have different technical requirements. For example, Internet telephony is sensitive to delay, but e-mail is not, so an ISP could give low delay to Internet telephony, but not to e-mail.

[11] C. Bastian et al., Internet Eng'g Task Force, RFC 6057, Comcast's Protocol-Agnostic Congestion Management System 23 (Dec. 2010), https://tools.ietf.org/html/rfc6057.
[12] See, e.g., Mosaic Telecom (2011); HardyNet (2015); Telispire (2014); Carolina West Wireless (2011); Wireless Hometown (2011); Anderson (2008).
[13] van Schewick (2015a), section "Problem 3".

Whenever an ISP has the power to speed up certain applications or slow down others, it might use this power to give certain applications an advantage over others. The proposal tries to mitigate this danger by forcing ISPs to consider an application's technical requirements when making distinctions among traffic.

However, this kind of class-based discriminatory network management still allows ISPs to give some applications an advantage over others, whether intentionally or inadvertently. It distorts competition, slows all encrypted traffic, harms individual users, stifles innovation, and creates high costs of regulation.

Allowing ISPs to treat classes differently gives them power to deliberately distort competition.

When ISPs are free to define classes, they have a lot of discretion to discriminate against certain applications. ISPs could use this power to deliberately distort competition. For example, an ISP could offer low delay to online gaming to make it more attractive, but it could decide not to offer low delay to online telephony because that would allow Internet telephony to better compete with the ISP's own telephony offerings. Although both services are sensitive to delay, ISPs could argue that there are other, technical differences that justify distinguishing between them.

Class-based traffic management can inadvertently harm applications.

Traffic management that distinguishes among different kinds of applications often results in inadvertent discrimination that hurts users, distorts competition, and makes it harder for providers of affected applications to innovate. Traffic management technologies that distinguish among classes of applications often end up harming certain applications, even if that effect is not intended, because the ISPs or their technology misclassify certain applications.

For example, many ISPs in the UK limit the bandwidth available to peer-to-peer file sharing applications during times of congestion, arguing that these applications are not sensitive to delay. This creates huge problems for online gaming. ISPs use deep packet inspection technology to identify these applications, but the technology doesn't work very well: it has a hard time distinguishing between online gaming and peer-to-peer file sharing, so online games stop working or don't work as well as they could. In the end, UK ISPs and gaming providers established standing committees where ISPs, technology vendors, and gaming providers worked together to make sure the games would work on ISPs' networks in spite of the discriminatory network management.

In the UK, this class-based traffic management not only creates problems for online gamers and gaming providers, whose applications perform worse than other kinds of applications, but it also creates problems for innovation. If an online gaming provider wants to introduce a new feature for its game in the UK, it needs to work with the ISPs and their technology vendors to make sure that the feature won't be caught up in the traffic management measures directed at peer-to-peer file sharing. This is the opposite of innovation without permission.

Similarly, until 2010, many ISPs in Canada used deep packet inspection technology to single out all peer-to-peer file sharing applications and limit the amount of bandwidth available to them

from 5pm to midnight. Again, ISPs assumed that it was alright to target peer-to-peer file sharing, because it's not sensitive to delay. But this assumption turned out to be wrong: there was an application called Vuze that used peer-to-peer file sharing protocols to stream video in real time. Real-time video is highly sensitive to delay, so the performance of Vuze suffered in the evening, when everybody wants to use the Internet.

Thus, the class-based traffic management might result in harmful discrimination by even the best-intentioned ISPs.

Class-based traffic management discriminates against encrypted traffic.

If traffic is encrypted, then the ISP cannot identify what kind of application—e-mail, telephony, web browsing—that a user is using, so it doesn't know what kind of treatment it needs. In the past, ISPs have addressed the problem by simply putting all encrypted traffic in the slow lane. That means that any time someone sends encrypted data, it will take longer to transmit. People encrypt their data for a variety of valid reasons, for example, to protect privacy, secure sensitive financial transactions, protect trade secrets, and guard against surveillance. If all encrypted data is automatically slowed down, it would discourage people from using encryption at all.

Class-based traffic management harms individual users.

Class-based traffic management takes the power to choose the right kind of service out of the hands of users and puts it into the hands of ISPs. However, people have different needs for speed on the Internet, and the same person has different needs at different times. As a result, a user's needs may differ from an application's technical requirements, so ISPs don't necessarily know what kind of service a user needs. For example, Internet telephony applications like Skype benefit from low delay, so ISPs may opt to give them low-delay service. That's great if you are doing a job interview, where you want the best quality possible. But if you are talking with a friend, you don't need crystal clear quality over Skype, so low-delay service might not be necessary. File uploads are generally considered not to be sensitive to delay. If you are uploading your hard disk to the cloud to do a backup, you will not mind that ISPs give file uploads lower priority. But if you are a student uploading homework right before it's due, or a lawyer filing a brief before the deadline, or an architect submitting a bid, then the speed of this upload is your highest priority. As long as ISPs, and not users, have the power to decide which classes of application get what kinds of service, users will never get exactly what they need. That's why class-based discrimination often harms users.

Class-based traffic management stifles innovation.

Imagine you develop a new application that would benefit from a specific kind of service. Entrepreneurs and start-ups typically do not have the resources or capacity to reach out to ISPs around the European Union to alert them that their particular application needs a certain kind of service. Even if a start-up manages to contact ISPs, they may not be interested in changing their systems for particular applications, which is a lot of work, especially when new apps don't have any users yet. Entrepreneurs should be able to get the kind of Internet service their application needs without having to seek ISPs' permission.

Class-based traffic management leads to high costs of regulation.

If ISPs get to define classes of applications, the only way to challenge these definitions is to complain to regulatory agencies. The agency would need to determine whether kinds of traffic are similar enough to be treated in the same way, a messy and costly process that would involve lots of lawyers and expert witnesses. This not only creates high costs of regulation, but also tilts the playing field against anybody—users, start-ups, small businesses, low-cost speakers—who doesn't have the money to engage in long and costly proceedings before a regulator." (End of Excerpt)

The social costs of discrimination among classes of applications are discussed in more detail in the attached paper "Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like."[14]

The attached article by Cooper and Brown provides vivid examples of how class-based traffic management in the UK harmed applications.[15]

The attached paper by Yiakoumis, Yiannis, Sachin Katti & Nick McKeown. 2016, describes the problems with DPI and the high transaction costs imposed by these services (pp. 3-4) and provides concrete evidence that user preferences are indeed heterogeneous (p.3).

References

Anderson, Nate. 2008. "WiMAX networks: we won't single out P2P for punishment." *Ars Technica.* http://arstechnica.com/uncategorized/2008/10/wimax-traffic-management-to-be-application-agnostic/

Bastian, C., T. Klieber, J. Livingood, J. Mills & R. Woundy. 2010. "Comcast's Protocol-Agnostic Congestion Management System." Request for Comments 6057. IETF.

Bretton Woods Telephone Company. 2011. "Network Management." *Bretton Woods Telephone Company.* http://bwtc.net/networkmanagement

Canadian Radio-Television and Telecommunications Commission. 2009. "Review of the Internet Traffic Management Practices of Internet Service Providers. Telecom Regulatory Policy". CRTC 2011-657. http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm

Carolina West Wireless. 2011. "Open Internet Policy." *Carolina West Wireless.* https://www.carolinawest.com/open-internet-policy/

Comcast. 2015. "Understand congestion management on our network." *Comcast.* February 11. http://customer.comcast.com/help-and-support/internet/network-management-information/

Cooper, Alissa & Ian Brown. 2015. "Net Neutrality: Discrimination, Competition, and Innovation in the UK and US." *ACM Transactions on Internet Technology*, 15(1): Article 2.

Federal Communications Commission. 2014. "Open Internet Roundtable - Policy Approaches." September 16. https://www.fcc.gov/news-events/events/2014/09/open-internet-roundtable-policy-approaches

[14] van Schewick (2015b), pp. 105-124.
[15] Cooper & Brown (2015), pp. 2:9-2:17.

Frischmann, Brett M. & Barbara van Schewick. 2007. "Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo." *Jurimetrics Journal*, 47(4): 383–428.

Frontier. 2015. "Network Management Policy." *Frontier*. https://frontier.com/networkmanagement/

Geist, Michael. 2007. "ISP Must come Clean on 'Traffic Shaping'." *The Star*. April 16. http://www.thestar.com/sciencetech/article/203408

HardyNet. 2015. "HardyNet Network Management Practices Policy Disclosure." *HardyNet*. February. http://hardynet.net/wp-content/uploads/2015/02/HardyNet-Network-Management-Policies-Disclosure-4-13-Ver.-3b-CURRENT.pdf

Lightstream. 2015. "Network Management Policy." *Lightstream*. http://www.lightstreamin.com/network-management-policy/

Meisner, Jeff. 2008. "Internet Congestion: ISPs Don Traffic Cop Uniforms." *ECommerce Times*. October 18. http://www.ecommercetimes.com/story/64861.html

Mosaic Telecom. 2011. "Mosaic Telecom Open Internet Policy." *Mosaic Telecom*. November 20. http://www.mosaictelecom.com/termsandconditions/OpenInternetPolicy.html

Plateau. 2013. "Plateau Network Management Policy." *Plateau*. http://www.plateautel.com/legal_net_mgmt.asp

Schmidt, Sarah. 2012. "Complaints About Online Traffic Delays Accelerating, Says CRTC." *Canada.com*. January 12. http://www.canada.com/life/Complaints+about+online+traffic+delays+accelerating+says+CRTC/5986923/story.html

Telispire. 2014. "Internet Policy." *Telispire*,. http://www.telispire.com/support/internet-policy/

van Schewick, Barbara. 2007. "Towards an Economic Framework for Network Neutrality Regulation." *Journal on Telecommunications and High Technology Law*, 5(2): 329-391.

van Schewick, Barbara. 2015a. "Europe Is About to Adopt Bad Net Neutrality Rules. Here's How to Fix Them." *Medium*. October 22. https://medium.com/@schewick/europe-is-about-to-adopt-bad-net-neutrality-rules-here-s-how-to-fix-them-bbfa4d5df0c8#.xln6uf7oa

van Schewick, Barbara. 2015b. "Network Neutrality and Quality of Service: What a Nondiscrimination Rule Should Look Like." *Stanford Law Review*, 67(1): 1-166.

Wireless Hometown. 2011. "Open Internet Principles of Wireless Hometown." *Wireless Hometown*. http://www.wirelesshometown.com/8.html