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 27, 2020

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

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

I submit these reply 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 reply comments draw heavily on my existing writings on net neutrality. 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.

Overview

Traffic management needs to be narrowly focused on measures that further legitimate network management purposes.

Some commenters suggest an expansive definition of what constitutes traffic management, listing measures such as making sure that Internet access is child-friendly or technical measures that ensure the service provided has the characteristics sold to the user (e.g., limiting the speed to the contractually agreed maximum speed).

Such an expansive definition of traffic management is counter to the interpretation of the reasonable traffic management exception in other net neutrality regimes and is not consistent with prior TRAI decisions on net neutrality.

The exception for reasonable network management is not the hook that can justify any exception from the net neutrality rules that is "reasonable." It needs to further a legitimate network management purpose.

According to the FCC's 2015 Open Internet Rules, "A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices." As the FCC explained in the 2015 Open Internet Order,

> "216. For a practice to even be considered under this exception, a broadband Internet access service provider must first show that the practice is primarily motivated by a technical network management justification rather than other business justifications. If a practice is primarily motivated by such another justification, such as a practice that permits different levels of network access for similarly situated users based solely on the particular plan to which the user has subscribed, then that practice will not be considered under this exception."[4]

Under the net neutrality regime established by the FCC's 2015 Open Internet Order, practices that are motivated by business motivations (such as throttling traffic once a subscriber hits its data caps or the technical measures necessary to limit a subscriber's speed to the contractually agreed speed) do not constitute reasonable network management. They are only allowed if they comply with the actual net neutrality rules, such as the non-discrimination rule.

The European Union's net neutrality regime takes a similar approach. According to Art. 3(3), subparagraph 2, reasonable traffic management measures "shall not be based on commercial considerations." As BEREC's 2016 net neutrality implementation guidelines explain,

> "68. In the event that traffic management measures are based on commercial grounds, the traffic management measure is not reasonable. An obvious example of this could be where an ISP charges for usage of different traffic categories or where the traffic

[4] FCC 2015 Open Internet Order, para. 216.

> management measure reflects the commercial interests of an ISP that offers certain applications or partners with a provider of certain applications."[5]

A legitimate network management purpose is "to maintain, protect, and ensure the efficient operation of a network." Network management includes, for example, managing congestion or protecting the security and integrity of a network, including addressing traffic that is harmful to the network such as denial-of-service attempts on network infrastructure elements.[6]

This interpretation is in line with the view of the reasonable traffic management exception in TRAI's 2017 recommendations and the license conditions. First, exceptions for other purposes are listed separately from reasonable traffic management (such as the exception for the provision of emergency services or the implementation of a court order). Second, reasonable traffic management measures are described as "transient." By contrast, technical measures designed to provide the contractually specified technical characteristics of a service are provided continually. Finally, allowing ISPs to contractually specify technical characteristics of their Internet access service that violate the net neutrality protections and then allowing them to justify the violation of these provisions as reasonable network management would allow them to easily circumvent the net neutrality protections just by specifying the violation in their description of the service, creating a gigantic loophole. Instead, the contractually agreed upon characteristics of a service need to be net-neutrality compliant.

As will be explained in the section on 5G below, this constraint still allows ISPs to offer Internet access services that are attractive to users and to differentiate their services from their competitors.

Finally, the kind of content-based filtering (e.g., to provide child-friendly Internet access) described by several commenters as a reasonable network management practice does not qualify as reasonable network management. It has no legitimate network management justification and therefore does not constitute traffic management, and it is not listed as a separate exception from the license condition's net neutrality requirements.

The net neutrality regime in Europe takes the same approach. First, Art. 3(3) of the regulation unequivocally prohibits ISPs from blocking or content filtering in the network. Filtering for parental control or content filtering in line with a user's wishes neither meets the requirements for reasonable traffic management under Art. 3(3) second subparagraph nor one of the exceptions the exceptions in Art. 3(3) third subparagraph (a)-(c). An exception related to parental controls and blocking unsolicited communications was deleted during the Trilogue negotiations, leaving no doubt about the legislative intent.

[5] BEREC 2016 Net Neutrality Implementation Guidelines, para. 68.

[6] See, e.g., van Schewick, 2015, Network Neutrality and Quality of Service, pp. 126-127; FCC 2015 Open Internet Order, paras. 220.

As the 2019 BEREC draft implementation guidelines clarify, this prohibition on blocking is non-negotiable and cannot be waived under Art. 3(2) as part of an ISP's agreement with an end user (see para. 37 of the draft guidelines).

Allowing ISPs to sell an IAS that includes blocks certain websites, applications, or services would also violate the regulation's ban on sub-internet offers (see paras. 17, 38, 55).

While prohibiting content-based filtering in the network, the European net neutrality regime still allows Internet users interested in content-based filtering to meet that need. That's because under the regulation, Internet users can use content-based filtering by installing endpoint-based filtering software on their computers or using other endpoint-based filtering solutions (see para. 78). This solution is preferable from a policy perspective. There are many competing providers of endpoint-based content filtering services, but Internet users generally can only choose among a few competing Internet access providers. The approach proposed here allows users to choose the filtering provider that fits their specific needs from the multitude of endpoint-based filtering services rather than forcing them to accept the specific content-based choices that their preferred Internet access provider would choose.

Explicitly requiring traffic management to be as application-agnostic as possible is necessary to prevent the harms to Internet users and providers of Internet applications, content, and services that net neutrality is designed to prevent.

In the absence of such an explicit requirement, ISPs have often engaged in network management practices that targeted specific applications or classes of applications.

Requiring network management to be only appropriate and tailored is not enough. The exception also must explicitly require network management to be as application-agnostic as possible. Otherwise, ISPs could justify network management practices targeting specific applications or classes of applications as a tailored, and therefore permissible, approach to managing congestion, as long as the discrimination is limited to times of congestion.

This would be a real problem. As experience from 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.

In Canada, the 2009 investigation of the CRTC into Internet service providers' network management practices showed that, at the time, many Canadian ISPs were singling out peer-to-peer file-sharing applications for special treatment, throttling the bandwidth available to them or interfering with these applications in other ways.[7] In the United States, Comcast, RCN, and,

[7] For an overview of Canadian providers' network management practices as disclosed during the proceeding, see CHRISTOPHER PARSONS, SUMMARY OF JANUARY 13, 2009 CRTC FILINGS BY MAJOR ISPS IN RESPONSE TO INTERROGATORY PN 2008-19 WITH FEBRUARY 9, 2009 UPDATES 15-31 (2009), *available at* http://www.christopher-

most likely, Cox for a while managed traffic on their networks by selectively interfering with BitTorrent and other peer-to-peer file-sharing applications but not with other applications.[8] In 2009, BT throttled streaming video of users subscribing to its "Up to 8 Mbps Option 1" broadband plan to 896 kilobits per second between 5:00 PM and midnight to manage congestion, limiting users' ability to watch video when most users would like to do so, while allowing the use of other applications that might be equally bandwidth intensive.[9] A recent study showed widespread discriminatory network management in the United Kingdom.[10] And according to NeelieKroes, who at the time was Vice President of the European Commission responsible for the Digital Agenda, data published by BEREC in June 2012 showed that around twenty percent of fixed Internet service providers (spread across virtually all EU member states) imposed restrictions on peer-to-peer file-sharing applications during peak times. These restrictions affected up to ninety-five percent of users in a country.[11]

parsons.com/PublicUpload/Summaryof_January_13_2009_ISP_filings_with_February_9_2009_Updates_version_1.0(for_web).pdf. Since then, most of the larger Canadian Internet service providers, most recently Bell Canada and Bell Aliant, 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. See Sarah Schmidt, Complaints About Online Traffic Delays Accelerating, Says CRTC, Canada.com (Jan. 12, 2012), http://www.canada.com/life/Complaints+about+online+traffic+delays+accelerating+says+CRTC/5986923/story.html; *see also* Michael Geist, Op-Ed., *ISP Must Come Clean on 'Traffic Shaping,'* THESTAR.COM (Apr. 16, 2007), http://www.thestar.com/business/2007/04/16/isp_must_come_clean_on_traffic_shaping html.

[8] Comcast Corp. Description of Current Network Management Practices, Letter from Kathryn A. Zachem, Vice President, Regulatory Affairs, Comcast Corp., to Marlene Dortch, Sec'y, FCC, Attachment A, Formal Complaint of Free Press & Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications, No. EB-08-IH-1518, Broadband Industry Practices, WC Docket No. 07-52 (Sept. 19, 2008), *available at* http://apps.fcc.gov/ecfs/document/view?id=6520172537; Comcast Corporation (2008), at 1, 9; RCN Corp., Ex Parte Notice at 1-4, Preserving the Open Internet, GN Docket No. 09-191, Broadband Industry Practices, WC Docket No. 07-52 (May 7, 2010), *available at* http://apps.fcc.gov/ecfs/document/view?id=7020450131.

RCN Corporation (2010), at 2, 4. Cox seems to have actively managed peer-to-peer filesharing in 2008 as well. Susan Davis, Cox About to Feel Wrath of Net Neutrality Activists, Wall St. J. Wash. Wire(May 15, 2008, 5:44 PM ET), http://blogs.wsj.com/washwire/2008/05/15/cox-about-to-feel-wrath-of-net-neutrality-activists (citing a Cox statement that "Cox allows the use of file-sharing and peer-to-peer services for uploads and downloads, and we allow access to all legal content, but we must manage the traffic impact of peer-to-peer services, as most ISPs do for the benefit of the customer" (internal quotation marks omitted)); Marcel Dischinger et al., Detecting BitTorrent Blocking, 2008 Proc.8th ACM SIGCOMM Conf. on Internet Measurement 3, 7-8(study finding evidence of BitTorrent blocking by Comcast and Cox).

[9] 9Rory Cellan-Jones, *iPlayer: BBC v BT*, BBC NEWS DOT.LIFE (June 2, 2009, 9:20 AM GMT), http://bbc.co.uk/blogs/technology/2009/06/iplayerbbc_v_bt html.See also Alissa Cooper, How Competition Drives Discrimination: An Analysis of Broadband Traffic Management in the UK (Aug. 2013) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2241562, at 21-22; and Alissa Cooper, How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and the United Kingdom chs. 5-7, at 105-211 (Sept. 2013) (unpublished Ph.D. thesis, University of Oxford), *available at* http://www.alissacooper.com/files/Thesis.pdf (same) (documenting widespread discriminatory network management in the United Kingdom).

[10] Cooper (2013a); Cooper, Thesis, Ch. 6, at 131-70.

[11] The text closely paraphrases European Commissioner NeelieKroes' description of these findings in her blog. NeelieKroes, Next Steps on Net Neutrality—Making Sure You Get Champagne Service if That's What You're Paying for, Eur. Commission Neelie Kroes' Blog (May 29, 2012), http://blogs.ec.europa.eu/neelie-kroes/netneutrality. For the detailed findings, see BEREC View of Traffic Management.

Discriminatory traffic management is just as harmful as blocking and discrimination for other reasons.

Some commenters suggest that ISPs should have broad flexibility to engage in discriminatory traffic management. This view seems to be based on the assumption that discriminatory practices are less harmful if they are used for traffic management.

This is not correct.

Discriminatory network management practices that single out specific applications or classes of applications significantly constrain users' ability to use the Internet as they like during peak times and make it more difficult for affected applications to reach their users. As online video company Zediva explained to the FCC in 2010,

> *Discriminatory network management of this type would put the affected applications at a severe disadvantage. Companies that offer these applications and services will be less able to reach their users during times of congestion, which in turn may affect their success in the market (who wants to use an application or service that is less usable during peak time, when most people actually want to use the Internet?) and their ability to get funding—thus squashing innovation before it has had a chance to prove itself in the marketplace.*[12]

Discriminatory network management also creates considerable collateral damage. In the UK, application-specific traffic management not only negatively affected targeted applications, but also interfered with applications like online gaming that the Internet service providers did not intend to target. This created considerable performance problems for affected applications. In response, application developers and network operators often had to expend significant resources to address these problems, and had to do so on an ongoing basis.[13] In addition, network management practices that single out specific applications or classes of applications for special treatment often motivate application developers to masquerade their applications to evade performance-reducing practices targeting their applications or to take advantage of performance-enhancing treatment provided to other applications, resulting in a cat-and-mouse game between network providers on the one hand and application developers and users on the other hand. Application-agnostic network management practices remove this incentive, freeing resources for network providers, application developers, and users.

Thus, application-specific network management practices are just as harmful as other forms of blocking and application-specific discrimination. For the user or provider of the affected application, it doesn't matter whether an ISP engages in blocking or discrimination to

[12] Ex Parte Letter of Zediva at 3-4, Preserving the Open Internet, GN Docket No. 09-191, Broadband Industry Practices, WC Docket No. 07-52 (Dec. 10, 2010), *available at* http://apps.fcc.gov/ecfs/document/view?id=7020923207.

[13] Ex parte http://apps.fcc.gov/ecfs/document/view?id=7521087920, Cooper (2013b), chapter 7, pp. 197-210.

increase its profits or manage its network. In both cases, users can't use the application of their choice, and application providers have problems reaching their users.

Simply requiring disclosure of traffic management practices is not enough to make traffic management measures "reasonable."

Some commenters seem to suggest that the only requirement needed to make traffic management measures reasonable is the disclosure of the practices to the consumer.

Several commenters seem to point to the experience with OFCOM's disclosure regime in the UK as an example of the success of this approach.

The opposite is true, both as a matter of theory and in practice.

Theory shows disclosure is not sufficient to protect consumers and providers of applications, content and services.

As I explain in detail in the attached article,[14] the argument that competition and disclosure are sufficient to protect consumers and providers of Internet applications, content, and services is based on the idea that if a network provider discriminates against an application that users would like to use, users can switch to another network provider that does not discriminate against the affected application. The threat of switching, proponents of this approach assume, will discipline providers.

In line with this reasoning, participants in the network neutrality debate often assume that the viability of disclosure rules as a substitute for substantive regulation solely depends on the amount of competition in the market for Internet access services. After all, if there is no competition, there will be no other providers that consumers can switch to in response to discriminatory conduct, making it impossible for them to discipline providers. Based on this reasoning, participants in the debate often assume that mandatory disclosure alone will be sufficient to discipline wireline providers in Europe or in countries like Canada, where the market for wireline Internet access is generally more competitive than in the United States. Similar arguments are often made for mobile Internet access, where users often have a choice between three or more competitors.

These arguments fail to recognize that the market for Internet services is characterized by a number of factors—incomplete customer information, product differentiation in the market for Internet access and for wireline and wireless bundles, and switching costs—that limit the effectiveness of competition and reduce consumers' willingness to switch. Rules that require network providers to disclose whether and how they interfere with applications and content on their networks reduce the problem of incomplete customer information, though only to some extent. They do not remove any of the other problems. As a result, they still leave the network

[14] van Schewick, 2015, Network Neutrality and Quality of Service, pp. 83-99.

provider with a substantial degree of market power over its customers, enabling it to restrict some applications and content on its network without losing too many Internet service customers. They also do not affect the cognitive biases, cognitive limitations, and externality problems that lead users to underestimate the benefits of switching providers compared to what would be in the public interest. Thus, even if there is competition in the market for Internet access services, disclosure cannot replace substantive regulation as a tool to discipline providers.

The available evidence shows disclosure is not sufficient to protect consumers and providers of applications, content and services.

The experience in Europe and Canada and in the market for mobile Internet services in the United States clearly demonstrates that competition and disclosure are not sufficient to discipline ISPs.

The markets for wireline Internet service in Europe and Canada are considerably more competitive than the market for wireline, fixed Internet services in the United States. The European legal framework does not prohibit restrictions on end users' use of applications or services, but it requires Internet access service providers to disclose them. Still, as the results of an investigation by the Body of European Regulators for Electronic Communications (BEREC) showed, many Internet service customers in the European Union were subject to restrictions on their fixed or mobile Internet services before the European Union adopted its 2016 network neutrality regulation.[15] A study by Cooper and Brown, described in more detail below, showed widespread discriminatory network management in the United Kingdom.[16] In Canada, the 2009 investigation of the CRTC into Internet service providers' network management practices showed that, at the time, many Canadian providers were singling out peer-to-peer file-sharing applications for special treatment, throttling the bandwidth available to them or interfering with these applications in other ways.[17]

Under the FCC's 2010 Open Internet Order, providers of mobile Internet services in the United States were subject to limited restrictions on their ability to block applications and were free to discriminate, but were required to disclose, among other things, blocking of or discrimination against applications.[18] Since the adoption of the 2010 Open Internet Order (and before the adoption of the 2015 Open Internet Order, which applied the same protections on mobile and fixed Internet access services), wireless carriers have engaged in various forms of discriminatory conduct, even though the market for mobile Internet services in the United States

[15] *A View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe: Findings from BEREC's and the European Commission's Joint Investigation*, BoR (12) 30 (May 29, 2012) [*BEREC View of Traffic Management*], *available at* http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/45-berec-findings-on-traffic-management-pra_0.pdf.

[17] Cooper (2013b), ch. 6, pp. 131-170.

[18] 47 C.F.R. § 8.3 (2014); *id.* § 8.5(a), *invalidated by* Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014); *see also Open Internet Order*, 25 FCC Rcd. 17,905, 17,938-39 (2010) (report and order) (describing the obligation to disclose "[a]pplication-[s]pecific [b]ehavior" under 47 C.F.R. § 8.3 (italics omitted)), *vacated in part*, *Verizon*, 740 F.3d 623.

is considerably more competitive than the market for wireline Internet services. Examples are Verizon Wireless's conduct towards tethering applications;[19] Verizon Wireless's, AT&T's, and T-Mobile's actions towards Google Wallet;[20] and AT&T's actions towards FaceTime.[21]

These examples suggest that—at least in the market for wireline Internet service in Europe and Canada and in the market for mobile Internet services in the United States—competition does not prevent Internet service providers from interfering with applications, content, or services on their networks, even if, as in the United States and the European Union, network providers are required to disclose any discriminatory conduct that occurs.[22]

Directly applicable to the topic of this proceeding, a detailed study of ISP traffic management in the UK from 2000 to 2010 by Alissa Cooper and Ian Brown exhaustively documents the failure of OFCOM's disclosure-based approach to adequately protect consumers and the providers of Internet applications, content, and service from ISPs' discriminatory traffic management practices.

First, they show in detail that despite the attention, energy and care that OFCOM put into requiring ISPs to disclose their traffic management practices, consumers either did not read these practices or did not understand them. As a result, disclosure did not actually empower consumers to adequately discipline provider. The relevant section of the article provides a vivid picture of the problems of this approach; I highly recommend reading it in full.[23] I attach the article to this submission.

Second, during the time covered by the study, most of the ISPs in the UK were using discriminatory traffic management practices that singled out specific applications or classes of applications for differential treatment. As Cooper's and Brown's article shows, this harmed not just the providers of the targeted applications and their users, who were unable use the internet as they wanted during peak times, but also many other applications such as online games or, in the case of Comcast in the US, Lotus Notes, that were inadvertently caught in these measures. As the article documents, ISPs in the UK were well aware of these problems, had to expend significant

[19] Barbara van Schewick, *Public Interest Requires Public Input: Verizon/Android Tethering*, INTERNET ARCHITECTURE & INNOVATION (June 30, 2011), https:// netarchitecture.org/2011/06/public-interest-requires-public-input-verizonandroid-tethering.

[20] Barbara van Schewick, *Is Verizon Wireless Illegally Blocking Google Wallet? It's Time for the FCC to Investigate*, INTERNET ARCHITECTURE & INNOVATION (Dec. 19, 2011), https://netarchitecture.org/2011/12/is-verizon-wireless-illegally-blocking-google-wallet-its-time-for-the-fcc-to-investigate.

[21] Cecilia Kang, *AT&T Faces Complaint over iPhone FaceTime Blocking*, WASH. POST POST TECH (Sept. 18, 2012, 9:08 AM ET), http://wapo.st/1yRD4ql; Chris Ziegler, *AT&T Only Allowing FaceTime over Cellular on Mobile Share Plans, No Extra Charge*, VERGE (Aug. 17, 2012, 4:29 PM), http://www.theverge.com/2012/8/17/3250228/att-facetime-over-cellular-ios-6-mobile-share.

[22] One could argue that the existence of restricted offerings is less problematic if there are unrestricted offerings available that users can switch to. As I have explained elsewhere, this argument is not correct. The restricted offerings harm users and reduce application innovation, even if unrestricted offerings are available. *See* Barbara van Schewick, Comments on the European Commission's Public Consultation on Specific Aspects of Transparency, Traffic Management and Switching in an Open Internet at 19-21 (Oct. 15, 2012), *available at* http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=3168.

[23] Cooper & Brown (2015), pp. 2:2-2:9.

time and resources trying to fix them and understood how much inadvertent harm these practices were causing to application developers. In addition, these problems created significant consumer backlash. However, in the absence of regulatory pressure to do so, the ISPs did not switch to application-agnostic traffic management measures, which would avoid these problems since they do not require ISPs to accurately identify specific applications or classes of applications. The relevant section of the article is full of detailed examples; I highly recommend reading it in full.[24]

By contrast, over the same period, ISPs in the US and, later, in Canada, were switching to application-agnostic traffic management measures in response to the FCC's 2008 Order against Comcast in the US and the CRTC Order on traffic management in Canada.[25] These ISPs were lauding the benefits of these practices in technical groups like the Internet Engineering Task Force, which develops the standards for the Internet.[26]

Thus, in spite of the significant amount of competition in the market for Internet access in the UK, OFCOM's disclosure-only regime failed to protect consumers and providers of Internet applications, content, and services. Instead, as the experience in the US and Canada shows, it was regulatory intervention that motivated ISPs to switch to application-agnostic traffic management.

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." DoT has integrated the exception with the requirements into ISPs' license conditions.

In my comments in this proceeding, I explained that net neutrality regimes in the US (pre-2018), the European Union and Canada have long required traffic management to be as application-agnostic as possible in order to qualify as reasonable network management. The requirement is also included in the California net neutrality law, which restores the 2015 net neutrality protections that had been in place at the federal level until 2018.

While TRAI's recommendations for net neutrality and the license conditions currently to do not explicitly mention this requirement, it is already implicitly included. That's because TRAI's recommendation and the license conditions require traffic management to be

[24] Cooper and Brown, pp. 2:9-2:17.

[25] See, e.g., the detailed description in Cooper (2013b), Chapter 5, and pp. 123-128 (describing ISPs' adoption of application-agnostic congestion management in response to the FCC's adoption of the 2008 Order against Comcast).

[26] See, e.g., Bastian, et al. (2010).

proportionate, and traffic management is only proportionate if it as application-agnostic as possible.

As I explained in my comments, this result follows directly from interpreting the license conditions in light of the goals of net neutrality. That's because the "application-agnostic as possible" standard allows ISPs to manage their networks while preserving user choice, competition, innovation, and free speech as much as possible. 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. At the same time, the exception provides a safety valve that allows network providers to react in more application-specific ways if a problem cannot be solved in an application-agnostic way.

TRAI would be in good company in adopting this interpretation: BEREC has already adopted this interpretation for the European net neutrality regime. According to BEREC, the requirement for traffic management to be proportionate requires the use of application-agnostic measures over application-specific measures as much as possible.

For example, as BEREC's 2016 net neutrality implementation guidelines explain, "when considering whether a traffic management measure is *proportionate*, NRAS should consider the following: […] There is not a less interfering and equally effective alternative way of managing traffic to achieve this aim (e.g. equal treatment without categories of traffic [BvS: i.e. application-agnostic traffic management]) with the available network resources."[27]

Similarly, the implementation guidelines make clear that even in cases of exceptional or temporary congestion under Art. 3(3), subparagraph 3(c), more application-specific measures of managing congestion are only allowed if application-agnostic measures are not sufficient, justifying this with the principle of proportionality.[28] And directly linking the need for congestion management to be as application-agnostic to the principle of proportionality, the guidelines go on to state:

> "92. Congestion management can be done on a general basis, independent of applications [BvS: i.e. using application-agnostic traffic management].[29] NRAs should consider whether such types of congestion management would be sufficient and equally effective to manage congestion, *in light of the principle of proportionality*. For the same reason, NRAs should consider whether throttling of traffic, as opposed to blocking of traffic, would be sufficient and equally effective to manage congestion." (emphasis added)

[27] BEREC 2016 Network Neutrality Implementation Guidelines, para. 61.

[28] BEREC 2016 Network Neutrality Implementation Guidelines, para. 90 and 91.

[29] BEREC Footnote 24, citing IETF, RFC 6057, Comcast's Protocol-Agnostic Congestion Management and IETF, RFC 6789, Congestion Exposure (Conex) Concepts and Use Cases.

In Europe, this requirement – that traffic management has to be as application-agnostic in order to be proportionate – applies both to traffic management measures under Art. 3(3), subparagraph 2 and 3(3), subparagraph 3 of the European Network Neutrality Regulation.[30]

TRAI should clarify that to be proportionate, traffic management measures should only be applied as long as necessary.

TRAI's recommendations on net neutrality and the license conditions already require traffic management practices to be "transient" in order to be reasonable. This suggests that TRAI envisions reasonable traffic management practices as measures that are limited in time and are activated in response to specific network management problems (as opposed to being in effect on an ongoing basis).

In addition, this interpretation directly follows from the requirement that traffic management needs to be proportionate.

As BEREC has explained, the principle of proportionality requires that traffic management measures should only be applied as long as necessary. For example, if the goal is to manage congestion, they should only be applied as long as there is congestion.

Under the European framework for net neutrality, the regulation explicitly requires that reasonable traffic management measures under Art. 3(3), subparagraph 2 "shall not be maintained longer than necessary." According to the BEREC implementation guidelines, "BEREC understands this term *as relating to the proportionality of reasonable traffic management measures in terms of duration*."[31]

Similarly, as BEREC explains, "[t]he three exceptions set out in Article 3(3) third subparagraph have as common preconditions that the traffic management measure has to be necessary for the achievement of the respective exception ('except as necessary') and that it may be applied 'only for as long as necessary'. *These requirements follow from the principle of proportionality*. Moreover, as exceptions, they should be interpreted in a strict manner."[32]

The same considerations are directly applicable to the interpretation of the reasonable network management exception in India. As an exception to the general net neutrality rules, the exception for reasonable network management needs to be interpreted narrowly. And the principle of proportionality requires that the network management is not applied longer than necessary.

The requirement that traffic management measures shall only be applied as long as necessary has long been part of the exception for reasonable network management exception in the US. Since the Order against Comcast, the FCC has required reasonable network management

[30] See BEREC 2016 Network Neutrality Implementation Guidelines, para. 61 and 90-93.

[31] BEREC 2016 Network Neutrality Implementation Guidelines, para. 72 (emphasis added).

[32] BEREC 2016 Network Neutrality Implementation Guidelines, para. 79 (emphasis added).

to be limited to times when the problem occurs.[33] Under the FCC's 2015 Open Internet Order, this requirement was viewed as part of the requirement that network management needs to be "tailored."

Creating an exhaustive list of reasonable traffic management practices in advance seems impossible. That makes it even more important for TRAI to specify more general requirements like the requirement for traffic management to be as application-agnostic as possible.

I share the skepticism expressed by many commenters that creating an exhaustive list of reasonable traffic management practices that do not violate the license conditions is not possible.

Whether a specific network management problem can be solved in an application-agnostic way will often be context-specific and may also depend on the network technology. For example, application-agnostic approaches that work well under normal conditions might not be suitable under rare conditions of exceptional network overload (e.g., after a natural disaster when the network infrastructure has suffered and everybody wants to use the Internet to contact their loved ones). Similarly, network engineers generally agree that while application-agnostic traffic management allows Internet access service providers to efficiently manage congestion on fixed networks, older cellular technologies like 2G may require more application-specific approaches.

Against this background, specifying the general requirement that traffic management needs to be as application-specific as possible is even more necessary to provide guidance to ISPs that will help them make decisions in specific circumstances.

TRAI should clarify that evaluations of traffic management practices under the "as application-agnostic as possible" standard will be based on the following hierarchy of traffic management practices.

The following hierarchy orders potential traffic management practices from least discriminatory to most discriminatory. Under the principle of proportionality, ISPs should only be allowed to

[33] FCC 2008 Comcast Order, para 48: "We next must ask whether Comcast's means *are carefully tailored to its interest in easing network congestion*, and it is apparent that no such fit exists. As an initial matter, Comcast's practice is overinclusive for at least three independent reasons. […] Second, *it is not employed only during times of the day when congestion is prevalent*: "Comcast's current P2P management is triggered . . . regardless of the level of overall network congestion at that time, and regardless of the time of day." And third, its equipment does not appear to target only those neighborhoods that have congested nodes — evidence suggests that Comcast has deployed some of its network management equipment several routers (or hops) upstream from its customers, encompassing a broader geographic and system area. With some equipment deployed over a wider geographic or system area, *Comcast's technique may impact numerous nodes within its network simultaneously, regardless of whether any particular node is experiencing congestion*." (emphasis added)

use a more discriminatory practice if less discriminatory practices are unable to address the network management problem in question.

- As a general rule, traffic management has to be as application-agnostic as possible. As explained above, requiring network management to be as application-agnostic as possible is good policy and necessary to preserve the ability of the Internet to serve as a level playing field as much as possible, while still giving ISPs the tools they need to manage their networks.[34]
- If a traffic management problem cannot be addressed in an application-agnostic way, ISPs may use traffic management measures that distinguish among classes of traffic based on objective technical requirements.
- If a traffic management problem cannot be addressed that way, ISPs are further allowed to make distinctions among classes of services provided similar classes of traffic are treated equally.
- If a traffic management problem cannot be addressed that way, ISPs are further allowed to make distinctions among individual applications.

At the same time, TRAI or DoT can and should provide guidance to ISPs that shows how the "as application-agnostic as possible" standard will generally apply to specific practices.

While it is not possible to conclusively specify the reasonableness of specific traffic management measures in advance given the context-specific nature of the standard, some general statements about specific traffic management practices are possible and would provide helpful guidance to ISPs.

TRAI should state that in general, it will not be reasonable to differentiate among applications or classes of applications to manage congestion on fixed networks, since fixed ISPs can manage congestion and provide a quality Internet experience for their subscribers in application-agnostic ways.

The experience of the past decade in the US and in Canada demonstrates that ISPs can generally manage congestion on fixed networks in application-agnostic ways. (As I explained in my comments in this consultation, ISPs in the US and Canada have been required to manage their networks in this manner since the FCC's 2008 Order against Comcast and the CRTC's 2009 Order on Traffic Management Practices).

[34] van Schewick (2015a), pp. 7-11 (discussing reasonable network management), 17-23 (discussing user-controlled Quality of Service and discrimination among classes of applications); van Schewick (2015b), pp. 137-140 (discussing reasonable network management), 124-133 (discussing application-agnostic discrimination), 133-137 (discussing user-controlled Quality of Service).

Network providers can enforce fairness among users and prevent aggressive users from overwhelming the network by allocating bandwidth among users in application-agnostic ways. During times of congestion (i.e., during times when a link's average utilization is high),[35] network providers may limit the amount of capacity available to users of that link based on application-agnostic criteria. A network provider could give one person a larger share of the available bandwidth than another, for example, because this person has used the Internet less over a certain period of time.

Even during times of congestion, network providers cannot, however, interfere with how users use the (limited) capacity available to them, for example, by selectively blocking or discriminating against specific applications or classes of applications. Thus, while the amount of bandwidth available to a user during times of congestion may be limited, users still get to decide how to use that bandwidth without interference from network providers.

To the extent that applications benefit from relative prioritization or other forms of differentiated treatment during times of congestion (i.e., during times when a link's average utilization is high), network providers could allow users to choose which applications to prioritize or otherwise treat differently during these times. As long as the option to be prioritized or be treated differently is offered equally to all applications or classes of applications (i.e., not tied or restricted to specific applications or classes of applications) and the choice of which applications to prioritize or treat differently is left to the user, this form of network management would be consistent with the reasonable network management exception proposed in my comments.

Tools for application-agnostic congestion management are available today. For example, Comcast, the largest provider of broadband Internet access services in the United States, adopted an application-agnostic congestion management system in response to the FCC's order against Comcast in 2008.[36] 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."[37] Thus, it is possible to protect the quality of the Internet experience of all Internet service customers in application-agnostic ways. Beyond Comcast's approach, vendors have developed network management solutions that allow the network provider to allocate bandwidth among users in an application-

[35] In discussions of the reasonable network management exception, the term "congestion" is generally used according to the definition of congestion used by network providers. Under that definition, congestion occurs if the average utilization of a link over a certain time period exceeds a certain threshold. *See* van Schewick, 2015, Network Neutrality and Quality of Service, Box 7.

[36] For descriptions of Comcast's application-agnostic network management system, see Comcast Corp. Description of Current Network Management Practices, Letter from Kathryn A. Zachem, Vice President, Regulatory Affairs, Comcast Corp., to Marlene Dortch, Sec'y, FCC, Attachment B, Formal Complaint of Free Press & Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications, No. EB-08-IH-1518, Broadband Industry Practices, WC Docket No. 07-52 (Sept. 19, 2008), *available at* http://apps.fcc.gov/ecfs/document/view?id=6520172537; Bastian, et al. (2010).

[37] Bastian, et al. (2010), at 23.

agnostic manner, while letting users choose the relative priority of applications within the bandwidth allocated to them.

Requiring traffic management to be as application-agnostic as possible is also compatible with new standards that are being developed by the Congestion Exposure Working Group in the Internet Engineering Task Force.[38] These standards would evolve the existing standards for the TCP/IP protocol suite in a way that allows the network provider to determine how much a user's traffic is contributing to congestion at any point in time. This information would allow network providers to manage their networks based on a user's contribution to congestion.[39] Network providers could use this information, for example, to allocate bandwidth among users during times of congestion based on their contribution to congestion, charge users based on their contribution to congestion, or count only traffic that contributes to congestion towards a user's monthly usage cap. Since a user's contribution to congestion is an application-agnostic criterion, all of these forms of differential treatment would be allowed under the proposed rule.

From a technical perspective, application-agnostic network management management has the added advantage of ending the arms race between application developers, users, and network providers that often develops in networks that use application-specific network management practices. Network management practices that single out specific applications or classes of applications for special treatment often motivate application developers to masquerade their applications to evade performance-reducing practices targeting their applications or to take advantage of performance-enhancing treatment provided to other applications, resulting in a cat-and-mouse game between network providers on the one hand and application developers and users on the other hand.[40] Application-agnostic network management practices remove this incentive, freeing resources for network providers, application developers, and users.

In light of this experience, the need for more application-specific congestion management would only arise in rare instances of exceptional network overload.

BEREC effectively adopted this approach in its 2016 network neutrality implementation guidelines. As explained above, the guidelines clearly explain that to be proportionate (one of the requirements for reasonable network management under the regulation), traffic management needs to be as application-agnostic as possible.

The guidelines couple this statement with more specific guidance related to congestion management, explaining that since application-agnostic congestion management is possible, that

[38] *See Congestion Exposure (CONEX): Charter for Working Group*, INTERNET ENGINEERING TASK FORCE, https://datatracker.ietf.org/wg/conex/charter (last visited Jan. 7, 2015).

[39] For an overview, see generally Arnaud Jacquet et al., *Policing Freedom to Use the Internet Resource Pool*, 2008 PROC. 2008 ACM CONEXT CONF.; and B. Briscoe et al., Internet Eng'g Task Force, RFC 6789, Congestion Exposure (ConEx) Concepts and Use Cases (Dec. 2012), https://tools.ietf.org/html/rfc6789.

[40] *See* van Schewick, 2015, Network Neutrality and Quality of Service, notes 269-72 and accompanying text.

should be the default, and adding that failure to properly dimension a network does not justify the use of more application-specific practices:[41]

> "Congestion management can be done on a general basis, independent of applications. NRAs should consider whether such types of congestion management would be sufficient and equally effective to manage congestion, in light of the principle of proportionality. For the same reason, NRAs should consider whether throttling of traffic, as opposed to blocking of traffic, would be sufficient and equally effective to manage congestion.
>
> As part of their scrutiny of congestion management practices, NRAs may monitor that ISPs properly dimension their network, and take into account the following:
>
> - if there is recurrent and more long-lasting network congestion in an ISP's network, the ISP cannot invoke the exception of congestion management (ref. Recital 15);
> - application-specific congestion management should not be applied or accepted as a substitute for more structural solutions, such as expansion of network capacity."

While mobile networks pose specific challenges, the expansion of capacity in more recent standards for cellular network technology suggests that it will often be possible to manage congestion in mobile networks using application-agnostic approaches, too.[42]

Thus, while 5G technology makes it easier for ISPs to differentiate traffic, the explosion in capacity reduces the need to do so.

TRAI should reject commenters' invitation to declare class-based traffic management practices as reasonable as long as they are based on the objectively different requirements of different technical quality of service requirements of specific categories of traffic.

Several commenters invite TRAI to declare class-based traffic management practices as reasonable as long as they are based on the objectively different technical quality of service requirements of specific categories of traffic.

TRAI should reject that invitation.

I agree with commenters that differentiating among classes of traffic based on the objectively different technical quality of service requirements of specific categories of traffic

[41] BEREC 2016 Implementation Guidelines, paras 92-93.

[42] See for example, the study by CTC Technology and Energy Consulting, Mobile Broadband Networks Can Manage Congestion While Abiding By Open Internet Principles. Study Prepared for the New America Foundation's Open Technology Institute – Wireless Future Project, https://static.newamerica.org/attachments/188-mobile-broadband-networks-can-manage-congestion-while-abiding-by-open-internet-principles/OTI_CTC_Wireless_Network_Neutrality_Engineering_Study_FINAL_111314.pdf.

(e.g., treating delay-sensitive applications differently from applications that are not sensitive to delay) is less discriminatory than differentiating among classes of traffic using other criteria such as the type of application (e.g., treating online gaming differently from online telephony, even though both are sensitive to delay), which in turn is less discriminatory than distinguishing between applications of the same type (e.g., treating one online video service differently from another). The hierarchy of traffic management measures listed above is based on this insight.

However, while different applications often have different quality of service requirements, even applications that are more sensitive to delay or have other more stringent requirements generally function well under application-agnostic traffic management in today's Internet. This applies, for example, to online telephony, online video conferencing, online video, or online gaming. Thus, it is generally not necessary to give them special treatment to provide a high quality user experience.

At the same time, these proposals ignore the significant social costs associated with class-based traffic management, even when the traffic management is supposed to be based on the objectively different technical quality of service requirements. My comments already discussed many of these costs.

Here, I want to focus on some of the additional problems associated with these practices.

In particular, while this approach sounds deceptively simple and clean in theory, it is almost impossible to implement in practice.

In order to make class-based differentiation work, ISPs have to continuously figure out how to classify all apps into categories, which is a Herculean task. Then they have to violate users' privacy by looking at every packet to see what apps they are using. (That's why the European net neutrality regime rightly prohibits the use of Deep Packet Inspection to do so.)

Even worse, there is no technology that allows ISPs to automatically identify and classify the content, applications, and services on an ISP's network, let alone their objective technical requirements. Deep packet inspection technology constantly misclassifies apps, and since the internet is now HTTPS and encryption by default, routers cannot look deeply into a packet to determine what it is. Remaining workarounds like DNS-snooping are closing.

That means many apps would not get the service they need and could even be put into buckets that harm them. As the Cooper and Brown article showed, we saw this in the UK, when games often stopped working in the evening, because ISPs were identifying them as peer-to-peer file-sharing applications, which the ISPs were throttling.

Moreover, the inevitable misclassifications require lots of work by both carriers and app makers to monitor and fix these problems. Again, the Cooper and Brown article documents this vividly.

Only the largest ISPs and the largest apps can afford to engage in this work; smaller apps will fall through the cracks.

The experience with zero-rating in Europe shows that these are not hypothetical concerns. The European net neutrality regime evaluates zero-rating case-by-case. While the BEREC 2016 net neutrality implementation guidelines suggest that zero-rating some apps in a category and requiring applications to pay to be zero-rated is likely to violate the guidelines, the guidelines are less clear on zero-rating offers that are open to whole categories of applications and do not require payment from edge providers to be included in the zero-rating program.

Like class-based traffic management based on objectively different technical requirements, these zero-rating plans sound less harmful than plans that differentiate among applications within a class by zero-rating only a subset of applications in a category.

However, since there is no automatic way for an ISP to identify applications or classes of applications on its network, ISPs establish strict technical standards as a condition for joining these programs. These standards favor applications that are easier to identify. They often discriminate against providers that use privacy-protecting encryption and innovative technologies.[43]

Services have to spend time and money to work closely with carriers on traffic identification and work with them again whenever they make changes to their service. That's hard for everyone, but impossible for many startups, small players, and non-commercial speakers.

Even getting in is hard for smaller players. AudioMack, a music application that is growing rapidly in the U.S., wanted to get a foothold in the E.U. With a staffer devoted full-time, the compay looked into 16 zero-rating plans for music; after six months of work, it was able to launch on just one. Meanwhile, Apple Music is part of all 16 plans.[44]

Research by Epicenter.works shows AudioMack isn't alone.[45] The research team tried to apply as a fake online service to 62 zero-rating offers they identified in 14 EU countries, but they were able to find only 18 points of contact. When they contacted them, they got only 8 responses within a month; 10 providers didn't even reply.

The administrative and technical burden of participating in zero-rating plans is so substantial that even app providers that manage to break into the zero-rating club can only handle

[43] For a detailed analysis of this problem based on T-Mobile's Binge On program in the US, e.g., https://cyberlaw.stanford.edu/downloads/vanSchewick-2016-Binge-On-Report.pdf, Section IV, pp. 17-28 (discussing the T-Mobile's technical requirements for inclusion in Binge On and the impact of these requirements on smaller application providers).

[44] https://berec.europa.eu/files/document_register_store/2019/5/3-c_Selfie-Networks_20190529_BEREC.PDF.

[45] https://epicenter.works/sites/default/files/2019_netneutrality_in_eu-epicenter.works-r1.pdf.

being part of a few zero-rating programs. As Epicenter.works has shown, the majority of apps that are zero-rated in Europe participate in at most three zero-rating plans.[46]

Only the largest companies have the resources and clout to fully take advantage of these programs. According to Epicenter.works, of the top 20 zero-rated apps in the E.U. only 3 are from the E.U.[47] The two-most zero-rated apps? WhatsApp and Facebook.

Thus, even zero-rating plans that are open to all apps in a category create lasting barriers for startups, smaller players, and commercial speakers, harming competition, innovation, and free speech.

TRAI rightly prohibited such class-based zero-rating programs, allowing only application-agnostic zero-rating. As a result, India has avoided these problems.

Instead, the Indian approach to zero-rating channels carriers' creative energies towards interesting application-agnostic zero-rating and application-agnostic pricing. Entrepreneurs can focus on developing their apps, rather than fighting to get into zero-rating programs.

The same problems will apply to class-based traffic management, whether based on objectively different quality of service requirements or not. Identifying applications correctly will be difficult, but many smaller providers of innovative content, applications, and services will not have the resources to work with many different ISPs to ensure they are correctly classified.

Even if they are be able to do so, the experience with zero-rating programs shows that ISPs often prioritize working with larger, established providers to ensure they are correctly identified and can be included in the program. Many smaller providers have to wait much longer or never hear back at all, hurting their ability to compete with larger, more established competitors.[48]

In short, allowing ISPs to differentiate among categories of traffic based on objectively different categories of traffic is not necessary, technically impossible and harms privacy and innovation.

While such measures may still constitute reasonable network management if the network management problem cannot be addressed in an application-agnostic way, in light of the significant harms associated with these practices it would not be proportionate to allow ISPs to engage in these practices if application-agnostic traffic management measures can solve the problem. Fortunately, the increase in capacity in 4G and 5G networks will make application-agnostic traffic management more feasible even on mobile networks.

[46] Ibd.

[47] Ibd.

[48] In addition to the experiences of AudioMack and Epicenter.works cited above, see, e.g., the experience with Music Freedom in the US. https://cyberlaw.stanford.edu/downloads/vanSchewick-2016-Binge-On-Report.pdf, pp. 26-28.

The European net neutrality regime only allows ISPs to engage in class-based traffic management based on objectively different requirements of the traffic if the traffic management problem in question cannot be addressed by application-agnostic measures.

Declaring that class-based traffic management based on objectively different technical requirements of the traffic constitutes a reasonable traffic management practice would run counter to the European net neutrality regime.

Observers sometimes assume the European net neutrality regime generally allows ISPs to differentiate among different classes of traffic based on objectively different requirements of the traffic. This interpretation is often tied to Recital 9 of the regulation, which clarifies that "[t]he requirement for traffic management measures to be non-discriminatory does not preclude providers of internet access services from implementing, in order to optimize the overall transmission quality, traffic management measures which differentiate between objectively different categories of traffic. "

However, this assumption is based on a misunderstanding of the European framework. It ignores the fact that to be reasonable under Art. 3(3), subparagraph 2, such measures still need to meet the other requirements established by Art. 3(3), subparagraph 2. As discussed above, these other requirements include the need for traffic management to be "necessary" and "proportionate."[49]

If a quality user experience can be provided using application-agnostic traffic measurement measures, differentiating among classes of traffic based on objective technical requirements is not "necessary." Yes, different apps have different needs. Email can handle delay, but not missing packets, while online calls can handle missing packets, but are more delay-sensitive.

However, that's much less relevant than one might assume. Both email and online calls function well on the normal internet. The same is true of online video and online games.

Thus, while there are applications that might *benefit* from special treatment, that does not mean that special treatment is *necessary*.

Moreover, as BEREC explicitly points out in para. 61 of the implementation guidelines, class-based traffic management is only "proportionate" if "there is not a less interfering and equally effective alternative way of managing traffic to achieve this aim (e.g. equal treatment without categories of traffic [BvS: i.e. application-agnostic traffic management]) with the available network resources."

[49] See Art. 3(3), subparagraph 2: "In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate …" and BEREC 2016 Network Neutrality Implementation Guidelines, para. 61 (explaining that a practice is only proportionate if it is necessary).

5G does not require a reconsideration of net neutrality in India.

Several commenters suggest that 5G technology is incompatible with net neutrality or requires a reconsideration of India's net neutrality protections. I disagree.

It seems the compatibility of 5G and India's net neutrality protections is outside the scope of this proceeding, and the question would merit its own consultation.

Still, I would like to provide a brief response to these arguments.

5G (the next generation of wireless technologies promises) speeds as high as 20Gbps with latency as low as one millisecond. Cell sites will also be able to handle many more devices connecting to them.

Simultaneously, 5G gives ISPs more ability to differentiate between apps and to wall off different parts of the network from others – sometimes referred to as network slicing.

Some commenters argue that India's net neutrality protections unduly limit Internet access service provider's ability to use this new technology.

But this is not really a new question. Meaningful net neutrality regimes already allow "good" discrimination and prohibit "bad" differentiation, and these distinctions are just as valid in a 5G world.

Technology that allows ISPs to differentiate traffic already exists, and net neutrality regimes around the world have always had to grapple with the question of how to separate good from bad differentiation. 5G just makes it easier for carriers to differentiate traffic, even as the explosion in capacity reduces the need to do so.

The existing framework already allows ISPs to use 5G technology to engage in socially beneficial differentiation.

Differentiation between different Internet access services

ISPs already sell different Internet access services with different technical characteristics at different prices. For example, different plans might have different maximum speeds or different data caps.

From a net neutrality perspective, these plans are not a problem. They offer the same type of service to each data packet transported under the plan; the treatment of data packets does not differ depending on the applications or classes of applications a subscriber is using. As a result, these plans do not interfere with users' ability to use the applications, content, and services of their choice and do not allow ISPs to interfere with the competition among applications, content, and services on their network.

While plans with different data volumes or speed might involve technical restrictions, the technical restrictions necessary to implement them do not differentiate between applications or classes of applications. Data caps limit how much data an end user can use overall and the plans might limit the amount of bandwidth available once a user reaches their cap, but these limits are application-agnostic – they apply to all traffic equally and do not differentiate among applications or classes of applications. Similarly, providing internet access service with a contractually agreed upon maximum speed (e.g., up to 1,5 Mbps) involves technically limiting the amount of bandwidth available to a user to 1,5 Mbps, but does not discriminate among applications or classes of applications. Similarly, charging a higher price for internet access service with a higher speed or a higher cap does not involve distinctions among applications or classes of applications.

By contrast, an Internet access service provider that consistently provided different speeds to different applications or different classes of applications (e.g., online telephony data packets receive speeds up to 1 Mbps, while data packets carrying online video receive speeds up to 1,5 Mbps) would violate the prohibition on discriminatory treatment of traffic under Clause No. 2.5 (i) of the license conditions, and such a plan could not be contractually agreed on under Clause 2.5 (ii). (As explained above, the consistent use of discriminatory traffic management as part of the provision of Internet access service does not constitute reasonable traffic management under the exception for reasonable traffic management, since it is not based on a network management purpose, but on commercial considerations, and is not transient.)

5G technology could allow ISPs to further differentiate their offerings by adding an additional dimension to the characteristics provided by a specific Internet access service plan.

For example, in addition to selling different Internet access services with different speeds and data volumes, ISPs might sell plans that have different Quality of Service characteristics such as latency (i.e. delay), jitter (i.e. variability of delay), or packet loss. For example, in addition to existing plans, an ISP might sell a premium plan that guarantees ultra-low delay and market it to avid gamers. The same provider could sell plans with guaranteed uptime Service Level Agreements, marketed to businesses.

While the specific quality of service characteristics might differ among plans, all data packets transported under such a plan would still receive the same type of service with the characteristics of that plan. In other words, like the Internet access plans already on the market, these new plans would still offer the same type of service to each data packet transported under the plan; however, unlike existing plans, the single type of service offered by the plan might no longer be best-effort service, but have different quality of service characteristics, e.g., providing lower delay or a guaranteed bandwidth.

From a policy perspective, these plans are not a problem because all the data in a particular plan receives the same treatment. The plans do not pick and choose among applications, and a user can choose the plan that best fit their needs.

They also would not violate the license conditions. Since each data packet sent by a specific customer receives the same service with the quality of service characteristics associated with that customer's plan, the technical measures applied to the data packets to create a service with these characteristics do not discriminate between applications or categories of applications. They do not violate the nondiscrimination provision and would not violate the ban on entering into agreements that result in discriminatory treatment of content.

Importantly, the license conditions do not allow ISPs to limit the use of such a plan to specific applications or classes of applications. In other words, the single type of service offered by the plan needs to be offered and provided in an application-agnostic way. Thus, an ISP can offer an Internet access service plan that provides lower delay than the normal best-effort service to all packets sent and received under the plan, but it cannot prohibit end users from using this plan for online telephony, nor can it technically limit the use of the plan to online games only. Such restrictions would violate the ban on blocking and on discrimination among applications or classes of applications.

Finally, if ISPs are allowed to offer different kinds of service with different quality of service characteristics, there is a danger that the provision of premium, higher-priced plans might degrade the quality of other, lower-priced Internet access subscriptions below the contractually specified conditions. To prevent this from happening, ISPs would have to properly disclose the technical characteristics of the service that a consumer can expect to receive under each plan, and the entity in charge of enforcing the license conditions would have to ensure that there is enough capacity and the network is managed in a way that ensures an adequate level of quality for all plans.

The ability to offer these kinds of Internet access plans is not tied to any specific advancement in technology; how ISPs implement such offerings is up to them. They could use technological capabilities provided by 5G. For example, different Internet access services with different quality of service characteristics might be implemented using different network slices. But ISPs could also use existing technology such as the IETF’s differentiated services for quality of service.

Differentiation between Internet access service and specialized services

The license conditions contain an exception for so-called specialized services that are offered separately from internet access. Specialized services are not subject to the license conditions’ protections against blocking, slowing down, and charging apps for fast lanes to the ISP’s subscribers.

Around the world, Internet access providers have argued that they want to use 5G technology to offer special treatment under the specialized services exception to any app that pays them a fee, and some commenters in this proceeding seem to suggest the same.

But that’s not what specialized services are for; they are supposed to be for apps that simply can’t work on the normal internet.

There will be some applications whose needs are so stringent that they cannot be met by normal internet service.

Take, for instance, remote surgery, where a specialist in France can perform neck surgery on a patient in Luxembourg. This is not a case for normal internet service, and the need for a dedicated 5G network slice or some other special treatment is obvious.

Allowing these kinds of applications to be offered as a specialized service protects innovation and allows applications to emerge that could not exist otherwise.

But if everything can be offered as a specialized service, this would circumvent the license conditions' ban on charging edge providers for a fast lane to the ISPs' subscribers.

That would be a huge problem. The license conditions ban ISPs from selling websites a fast lane to the ISP's customers because they tilt the internet in favor of deep-pocketed incumbents, hurting startups, non-profits, NGOs, and small businesses that cannot afford to pay.

Allowing ISPs to move applications off the normal internet at will to give them special treatment would also break the virtuous cycle between improvements in applications and subsequent improvements in the network.

Years ago, people argued that online calling, online video, and real-time data would be impossible to deploy without special treatment from the network.

All of these proved to be false. App makers figured out how to make these services work on lower-bandwidth connections, and demand for these services drove investment in network upgrades. Once new capacity was created, application developers invented new uses for that capacity. They could do so, because this capacity was not limited to companies with deep pockets that can pay for special treatment.

This is the virtuous cycle in action.

By contrast, if ISPs had been able to shunt online voice, video, and real-time data into specialized services, they would have created a very different world that would have required app providers to pay ISPs.

That would have slowed innovation, impeded the emergence of competitive apps, raised prices for end users, and made free apps untenable.

Thus, net neutrality regimes that strike the right balance allow the provision of specialized services for applications that truly cannot function on the normal internet, while prohibiting it for those that can.[50]

[50] In a limited exception to this rule, fixed and mobile network operators should continue to be allowed to provide special treatment to their own IP-based traditional telephony services (e.g., VoLTE offered by cellular carriers); fixed network operators should continue to be allowed to provide special treatment to their own traditional linear broadcasting IPTV services. They should be grandfathered in as specialized services to account for these operators' reliance interests. Online telephony and online video can function on the normal Internet, so without this exception

The advent of 5G does not change this fundamental trade-off. Just because 5G technology makes creating specialized services easier, that does not mean we should build a new, less open world out of them.

TRAI should clarify that an optimization is not "necessary in order to meet specific quality of service requirements" if the application or service in question can function on a well-provisioned Internet access service.

The license conditions ban ISPs from offering technical preferential treatment (so-called "fast lanes") to providers of normal Internet applications, content, and services in exchange for a fee (Clause 2.5 (ii)). There is a danger that ISPs could use the license conditions' legitimate exception for specialized services to circumvent that ban.

This is not a hypothetical threat. ISPs around the world continue to make clear that they want to use the specialized service exception to offer preferential treatment to everyday Internet application like online gaming, online telephony, video conferencing, or online video for a fee.[51]

To prevent any game-playing by ISPs, TRAI must state clearly how it will distinguish legitimate specialized services from attempts to circumvent the ban.

Fortunately, the existing license conditions already include the language necessary to reach that goal.

To reach this goal, TRAI should clarify that an optimization is not "*necessary* in order to meet specific quality of service requirements" if the application in question can function on a well-provisioned Internet access service. By contrast, the fact that an optimization improves the performance of an application compared to that application's performance on a normal internet access service does not make the optimization "necessary." Finally, if the application cannot function on the normal Internet, then it is a legitimate specialized service that can take advantage of the specialized services exception.

This interpretation flows from the wording of the license condition, the overall goals of the license conditions, and the overall structure of the conditions.

According to Clause 2.5(iv), "specialized service" means

- services other than Internet access services that are optimised for specific content, protocols, or user equipment,
- where the optimisation is necessary in order to meet specific quality of service requirements."

for these services offered by these operators, these services would fail to meet the requirements for a specialized service.

[51] See, e.g., Deutsche Telekom (2015).

The second part of this phrase is key for distinguishing between (a) a specialized service that circumvents the net neutrality rules and (b) a legitimate specialized service.

Different content, applications, and services have different requirements for specific levels of quality. For example, online telephony functions particularly well if one-way delay is less than 150 ms, and becomes effectively unusable if delay is larger than 400ms. One-way jitter should be below 30 ms. The amount of packet loss that an online telephony application can tolerate depends on the specific coding and loss-concealment techniques used and can reach from 1% to 20%. Streaming video applications that stream stored video can usually tolerate delays of several seconds. They don't have specific jitter requirements, but packet loss should not exceed 5 %.

In spite of having requirements for specific levels of quality, these applications generally function well on today's Internet access services. Thus, even though these applications have requirements for a specific level of quality, these requirements are being met by normal Internet access services. In these cases, an optimization is not "***necessary*** in order to meet specific quality of service requirements," and these applications do not meet the license conditions' requirements for specialized services.

By contrast, if an application has requirements for a specific level of quality that cannot be met by normal Internet access services, making it impossible for the application to function on those services, then an optimization is "***necessary*** to meet the requirements of the content, applications, or services for a specific level of quality."

This interpretation gives us exactly the results we need. If an application can function on the normal Internet, then allowing it to buy an optimisation as a specialized service would basically result in it paying for a fast lane, violating Clause 2.5(ii). But if the specialized service cannot function on the open Internet and meets the definition of optimization as necessary, this is precisely the kind of service for which the exemption was made. Under this interpretation, the specialized services exception allows those kinds of applications to emerge that could not exist otherwise.

This interpretation best realizes the goals of the license conditions. Interpreted this way, the specialized services exception enables innovation in applications, content, and services that could not exist in the absence of specialized services.

At the same time, this interpretation makes it impossible to use specialized services to circumvent the license conditions' ban on selling preferential treatment to providers of Internet content, applications, and services for a fee, which is critical to realizing the goals of the license conditions to protect Internet users and guarantee the continued functioning of the internet ecosystem as an engine of innovation and a platform for free speech.

Finally, this interpretation flows from the structure of the license conditions. First, as a general rule, exceptions (here: the specialized services exception) should be interpreted narrowly in order not to swallow the rule (here: the license conditions' ban on fast lanes). In addition, Clause 2.5(iii)(a) explicitly states that specialized services "shall not be usable or offered as a replacement for internet access services." From the perspective of both the end user and the application provider, a specialized service offering higher quality transmission to a normal Internet application "replaces" the transmission service provided by regular internet access and is therefore "usable" and "offered as a replacement for internet access services" with respect to this application, violating Clause 2.5(iii)(a).

This interpretation would provide the same level of protection as the European net neutrality framework. As BEREC explicitly stated in its 2016 net neutrality implementation guidelines, National Regulatory Agencies "should verify whether the application could be provided over IAS at the specific levels of quality which are objectively necessary in relation to the application, or whether they are instead set up in order to circumvent the provisions regarding traffic management measures applicable to IAS, which would not be allowed."[52]

When evaluating whether the application can function on the normal Internet, regulators should focus on the kind of application, not on the specific quality level at which it is offered.

When evaluating whether the application can function on the normal Internet, the entity enforcing the license conditions should focus on the kind of application, not on the specific quality level at which it is offered, and TRAI should state that explicitly.

Thus, offering online video at a higher definition or online telephony at a lower delay than currently supported in the normal Internet does not meet the requirements for a specialized service because online video and online telephony can function on the normal Internet.

In the past, ISPs have suggested that they should be allowed to offer specialized services to online video providers that make it possible to stream video at a higher resolution than currently common on Internet access services (e.g., 4K), even though online video can function effectively on the normal internet access service. Adopting this interpretation would essentially would treat standard definition video and high-definition video as two different applications when analyzing whether "the optimisation is necessary in order to meet specific quality of service requirements."

Such a result would directly circumvent the ban on selling fast lanes to providers for Internet content, applications, and services in Clause 2.5(ii). Selling better treatment to a specific application that can function on the Internet to an edge provider for a fee is the essence of such a ban.

[52] BEREC 2016 Network Neutrality Implementation Guidelines, para. 105. See also para. 111: "NRAs should verify whether, and to what extent, optimised delivery is objectively necessary to ensure one or more specific and key features of the applications, and to enable a corresponding quality assurance to be given to end-users. To do this, the NRA should assess whether an electronic communication service, other than IAS, requires a level of quality that cannot be assured over a IAS. If not, these electronic communication services are likely to circumvent the provisions of the Regulation and are therefore not allowed."

Increasing the resolution of a video or the quality of an application does not create a new application. It is the same application at different quality levels. This is supported by the fact that many of today's applications (e.g., online video or online telephony) dynamically adjust the resolution or bandwidth-intensity of the application based on the current conditions in the network. YouTube allows users to watch video at different resolutions, but it is still one application.

Treating different quality levels of the same application as one application instead of several is also required by the goals of license conditions. Offering a higher quality to an application that can function on the normal Internet is exactly the kind of fast lane that the license conditions were meant to prevent. Otherwise, the ban on fast lanes would be meaningless.

Treating different quality levels as different applications would also stop the virtuous cycle between improvements in applications and improvements in the network that has driven both innovation and investment in applications and in the network. The fact that an application has difficulties functioning at the current level of quality available on the Internet often motivates application designers to improve the application's technology so that it can work at the available level of quality. At the same time, innovations in Internet applications and services might create a need for additional network capacity. For example, the advent of online video applications increased customer demand for higher capacity Internet connections in the US, prompting US ISPs to invest in deploying additional network capacity in the last mile. Once that capacity was available, it not only benefitted online video applications, but opened up opportunities for other new uses of the Internet that might need that capacity.

If standard definition video does not qualify for a specialized service, but 4K video does because of its higher requirements, this creates an incentive for ISPs not to invest in additional capacity and instead channel 4K video services into specialized services, which allow the ISP to charge the content provider for the special treatment. This harms those video providers that would like to offer their video in 4K, but cannot pay extra fees for a specialized service (e.g., start-ups, small businesses, educational institutions, activists, or independent artists) and their viewers. It also harms the providers of other Internet applications, content, and services which would have been able to take advantage of the additional capacity had the ISP allocated it to normal Internet access instead of allocating it to specialized services. Any other interpretation would freeze in place the open Internet of today; everything that needs more would have to do it as a specialized service.

TRAI should make an exception from this definition for certain services offered by ISPs based on reliance interests.

In general, the interpretation proposed above provides the right results. However, in a limited exception to this rule, fixed and mobile network operators should continue to be allowed to provide special treatment under the specialized service exception to their own IP-based traditional telephony services (e.g., VoLTE offered by cellular carriers); fixed network operators should continue to be allowed to provide special treatment to their own traditional linear broadcasting IPTV services.

As the existence of numerous online telephony and online video services show, these applications could function on the normal Internet, and so they would fail the test set out above. However, banning these services now would frustrate legitimate reliance interests. Carriers have been allowed to offer these services in the past and have made investments (such as acquiring spectrum) with the expectation that they would be able to offer both mobile voice and Internet services over that connection, and TRAI and DoT should honor those expectations.

Creating an explicit, limited carve-out for these services is preferable over weakening the definition of "necessary" so that it would capture those services. In principle, these services are no different from other services that can function on the normal internet, so there are no other criteria that could be used to meaningfully distinguish them from specialized services that circumvent that ban. Thus, any definition of the word "necessary" that would allow these services to be offered as a specialized service would allow all Internet applications to do the same, opening a gigantic loophole that makes the license conditions' ban on fast lanes meaningless. The only reason to treat them differently is the reliance interest, so listing them explicitly as an exception is the best way to solve that problem.

Neither TRAI nor DoT should delegate the evaluation of traffic management measures to another entity.

Net neutrality protections are necessary because ISPs' private interests diverge from the public interest in a free and open Internet.

As I have explained elsewhere, net neutrality rules are necessary because network providers' decisions about whether, when, and how to engage in discrimination will not necessarily result in socially desired outcomes. Network providers are not beneficial stewards of the Internet platform. They are private actors that pursue their private interests. Network providers' private interests often differ from users' interests, and even if they do not, network providers do not know exactly what users want.[53] Network providers' private interests and the public's interests with respect to the evolution of the Internet diverge as well. It is this market failure that network neutrality rules are designed to address.[54]

For a variety of reasons, network providers capture only a small part of the social value resulting from an open Internet. For example, they capture only some of the social benefits

[53] See van Schewick, 2015, Network Neutrality and Quality of Service, notes 431-36 and accompanying text.

[54] For a detailed discussion, see van Schewick (2010), pp. 355-71 (describing the public interest); pp. 371-75 (describing network providers' private interests and why they diverge from the public interest).

associated with application innovation or resulting from improved democratic discourse.[55] Moreover, most of the gains they are able to capture are uncertain and will be realized in the future, which leads network providers to discount them even more.[56]

All of this makes it less likely that the decisions of an ISP-led body or even a multi-stakeholder body will reflect the public interest rather than the ISPs' private interests.

If TRAI or DoT decide to establish a multi-stakeholder body, this body should have a purely advisory capacity and would have to be structured carefully to prevent capture by ISPs or ISP-funded players.

I share the concerns about potential capture of a potential multi-stakeholder body by Internet access providers expressed in the comments by Mozilla and the Internet Freedom Foundation.

Avoiding such an outcome requires carefully structuring any multi-stakeholder body to ensure that all affected stakeholders are adequately represented and that ISPs do not have a majority. For example, the composition suggested by Mozilla would result in a more balanced composition.[57]

As Mozilla and others have pointed out, such a body should have a uniform category of memberships only and not require the payment of fees to participate or vote. Membership fees would establish barriers to participation for academics, civil society actors, small businesses and startups and would make participation impossible for many of them.

But even with such structural measures in place, the decision over the reasonableness of traffic management measures should remain the sole prerogative of TRAI or DoT.

References

Bastian, Chris, Tom Klieber, Jason Livingood, Jim Mills & Richard Woundy. 2010. "Comcast's Protocol-Agnostic Congestion Management System." *Internet Engineering Task Force (IETF)* December. https://tools.ietf.org/html/rfc6057

Comcast Corporation. 2008. *Comcast Corporation Description of Current Network Management Practices*. Attachment A to Comcast Corporation's Filing In the Matter of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications submitted September 19, 2008. WC Dkt. No. 07-52. http://apps.fcc.gov/ecfs/document/view?id=6520172537

Cooper, Alissa. 2013a. "How Competition Drives Discrimination: An Analysis of Broadband Traffic Management in the UK." Paper presented at 41st Research Conference on Communication, Information and Internet Policy (TPRC 41). Arlington, Virginia, USA.

[55] *Id.*, pp. 373-74; *see also* Frischmann (2005), pp. 1009-12; Frischmann & van Schewick (2007), pp. 400-03, 424-25.

[56] van Schewick (2010), pp. 374-75.

[57] Mozilla comments, p. 12.

Cooper, Alissa. 2013b. "How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and the United Kingdom." DPhil Thesis. Oxford University, Oxford, UK.

Cooper, Alissa & Ian Brown. 2015. "Net Neutrality: Discrimination, Competition, and Innovation in the UK and US." *ACM Transactions on Internet Technology (TOIT) - Special Issue on Foundations of Social Computing*, 15(1).

Deutsche Telekom. 2015. "Net neutrality: Finding consensus in the minefield." October 28. https://www.telekom.com/media/management_unplugged/291728

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

Frischmann, Brett M. 2005. "An Economic Theory of Infrastructure and Commons Management." *Minnesota Law Review*, 89 (April): 917-1030.

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.

RCN Corporation. 2010. Ex Parte Letter to Federal Communications Commission. GN Dkt. No. 09-191. May 7. http://apps.fcc.gov/ecfs/document/view?id=7020450131

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. 2010. *Internet Architecture and Innovation.* Cambridge, MA: MIT Press.

van Schewick, Barbara. 2015a. *The Case for Meaningful Network Neutrality Rules.* Attachment to Barbara van Schewick's Ex Parte in the Matter of Protecting and Promoting the Open Internet submitted February 20, 2015 to the Federal Communications Commission GN Dkt. No. 14-28. http://apps.fcc.gov/ecfs/document/view?id=60001031682

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