CENTER FOR DEMOCRACY & TECHNOLOGY

July 5, 2016

Mr. A. Robert J. Ravi
Advisor (QOS)
Telecom Regulatory Authority of India

Re: Pre-Consultation Paper on Net Neutrality

Center for Democracy & Technology Comments

Dear Mr. Ravi,

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the questions raised in the TRAI's pre-consultation paper regarding net neutrality. CDT is a nonprofit public interest organization dedicated to promoting openness, innovation, and freedom online—a mission that closely tracks the policy objectives mentioned in the 2015 DoT Committee report on net neutrality. CDT participated in the TRAI's consultation on differential pricing and applauds the TRAI's continued efforts to preserve open internet values for India. With regards to the questions presented in the pre-consultation paper, CDT offers the following responses:

Core Principles

The term "net neutrality," as originally coined by Tim Wu, refers to a network that remains neutral as to competition among applications at its endpoints.[1] Although this concept has broadened somewhat to account for the possibility of discrimination based on the content, sender, receiver, devices, or mode of communications used at the endpoints of networks, the core principle remains unchanged: network operators should not leverage their position to favor or disfavor what happens at the edges of their networks.

Discrimination of this sort runs counter to the principles that have made the open internet a vibrant platform for expression, a dynamic environment for innovation, and a robust and competitive marketplace.[2] The principles of innovation without permission, of equal access, and of open, undistorted competition enable tiny start-ups to succeed, give people unrestricted choices among information sources, applications, and markets, and provide equal opportunities for market entrants. But internet service providers are in a position to undermine these fundamental principles by blocking,

[1] Tim Wu, *Network Neutrality, Broadband Discrimination*, Journal of Telecommunications and High Technology Law, Vol. 2, p. 141 (2003).
[2] In the Matter of Protecting and Promoting the Open Internet, Comments of the Center for Democracy & Technology, 4 (2014), available at: https://cdt.org/files/2014/04/cdt-open-internet-comments-3-14.pdf.

throttling, or placing conditions on access to the open internet.[3] Whatever form future regulations may take, targeting this discrimination is essential to ensuring the neutrality of the internet.

Traffic Management

Traffic management is an essential function of network operators. In its most basic form, traffic management can consist of management signals sent over the network for the purpose of administration and maintenance of various types of computer and network hardware necessary for the network to function. In addition to basic infrastructural signaling, traffic management also refers to the practice of treating traffic differently, typically congruent to technical tolerances for the type of traffic being managed.[4] For example, traffic management signals used to configure and administer network hardware must be prioritized over traffic that the network is carrying since transmitting content over the network depends on the health and functioning of the underlying network. Traffic management can allow for more efficient utilization of network resources, improving the speed and efficiency of the network so that the end users' quality of experience is maximized even as networks approach capacity. Regardless of traffic volume, network operators must have some method to decide in what order their routers and switches should process packets arriving simultaneously. In some cases, it may be desirable to give certain kinds of traffic priority over other kinds. For instance, giving latency-sensitive traffic like Voice over Internet Protocol (VoIP) data priority over less sensitive traffic like web searches, file downloads, or email can improve the VoIP user's experience without negatively impacting the experience of the other uses at all. Indeed, many network operators have policies in place that govern such differential treatments.[5]

As an exception to a rule against differential treatment of packets, traffic management should be limited, but not rigidly prescribed, as flexible traffic management can be very important in providing the network transmission required for certain kinds of applications. Framing the exception in terms of the desired outcome of traffic management practices, rather than in terms of the specific practices themselves, could allow providers to implement innovative traffic management solutions without running afoul of a prohibition on discrimination. For instance, allowing network operators to treat packets differently to achieve objective technical specifications required for application functionality, provided that differential treatment remains agnostic to specific applications and does not materially

[3] See Verizon v. FCC, 740 F.3d 623, 645-46 (D.C. Cir. 2014)(affirming the FCC's determination that internet access providers "may be motivated to discriminate against and among edge providers" and that they have the "technological ability to distinguish between and discriminate against certain types of traffic," as well as the incentive to discriminate against unaffiliated traffic).
[4] Broadband Internet Technology Advisory Group, *Differentiated Treatment of Internet Traffic,* (2015), avialable at: https://www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf.
[5] *See, e.g.*, Frontier, Network Management Policy, https://frontier.com/networkmanagement/.

impact customer experience, may limit the possibilities for unwanted discrimination. However, as exceptions may be targets for abuse, network operators should be transparent as to any traffic management techniques or policies they employ. Finally, encryption should not be a basis for differential treatment.

Regulatory Approach

The diversity of regulatory approaches to protecting an open internet taken by the countries mentioned in the pre-consultation paper, as well as those not mentioned, demonstrates that the approach to regulation depends heavily upon the context in which those regulations will operate. CDT recognizes that the circumstances in India. as well as the TRAI's policy goals, may differ from other countries, and that the TRAI's chosen regulatory approach will reflect those differences. Irrespective of these differences, establishing clear rules against those practices, such as blocking, throttling, and paid prioritization, that are inimical to the principles of an open internet could provide a strong foundation on which to build future regulations. Such rules provide certainty for both service providers and customers and would complement the TRAI's regulation on differential pricing.

In addition to strong, clear rules against undesirable practices, the TRAI may wish to consider a broader, more flexible standard against which to judge any practices or conduct not encompassed by the rules. This approach would allow service providers to innovate outside of the prohibited practices while preserving regulatory oversight and authority to assess whether a service provider's practices or conduct conflicts with the fundamental policy goals.

Privacy

In a current rulemaking, the United States Federal Communications Commission (FCC) is considering what obligations ISPs have with respect to the information they collect about their customers.[6] One of the relevant statutes requires telecommunications carriers to "protect the confidentiality of the proprietary information of...customers."[7] The statute and the Commission's rulemaking recognize that there are important and innovative ways in which ISPs may make use of the customer information to which they have access because of the service they provide, but that customers should be empowered with both knowledge and choice as to how their carriers use that information. CDT suggests that the TRAI also consider the scope and sensitivity of the personal information service providers can access, as well as the importance of a customer's informed consent as to the use of that information. Our

[6] United States Federal Communications Commission, *In the matter of Protecting the Privacy of Customers of Broadband and other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (Apr.1, 2016).
[7] 47 U.S.C. § 222.

comments in the FCC's broadband privacy rulemaking may be useful as the TRAI considers these aspects of customer privacy.[8]

Internet service providers have access to a significant amount of personal and private information that can be related to individuals.[9] Although use of encryption technologies is becoming more common, those technologies may still leave some personal or private information exposed.[10] This is due, in part, to the structure of individual Internet Protocol (IP) packets, which contain several layers of unencrypted metadata outside the actual content of the packet, which may or may not be encrypted.[11] This packet metadata, especially when associated with other customer-specific information an ISP may have, like names and addresses, can be used to build comprehensive customer profiles and make detailed inferences about the online and offline behavior of individuals.[12]

ISPs can access even more detailed and sensitive information using technologies that enable them to look beyond packet metadata. This practice, sometimes called deep packet inspection (DPI), might be used by network operators to enhance their traffic management practices. DPI is not, however, necessary for network functionality. Given the privacy implications of DPI, CDT therefore recommends that such practices be discouraged, or in the alternative, only implemented after explicit approval by the customer.

Respectfully,

Stan Adams

---

[8] *In the matter of Protecting the Privacy of Customers of Broadband and other Telecommunications Services,* Comments of the Center for Democracy & Technology, ("CDT Broadband Privacy Comments") available at: https://cdt.org/files/2016/05/Broadband-Privacy-Comment-FINAL-word.pdf.

[9] Aaron Rieke, David Robinson & Harlan Yu, What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate 7, Upturn (March 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

[10] CDT Broadband Privacy Comments at 16-17.

[11] See Center for Democracy & Technology, *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (Jan. 20, 2016) ("CDT CPNI Chart"), https://cdt.org/insight/applying-communications-act-consumer-privacyprotections-to-broadband-providers/.

[12] CDT Broadband Privacy Comments at 16.