

To:

Shri R. M. Agarwal, DDG (NT),
Department of Telecommunications,
Ministry of Communications and Information Technology,
20, Ashoka Road, Sanchar Bhawan,
New Delhi- 110001

New Delhi, 20 August, 2015

Re: Response to the report on net neutrality released by the Department of Telecommunications Committee

Dear Shri R. M. Agarwal,

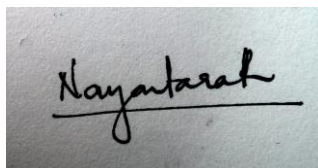
The Internet Democracy Project (www.internetdemocracy.in) is a Delhi-based civil society initiative that seeks to unearth the changes that Internet is causing in democracy, in India and beyond. We are writing to you with comments on the report on Net Neutrality released by the Department of Telecommunications.

We would be grateful if you could consider the concerns raised in our response and incorporate changes that may better serve public interest. The Internet Democracy Project was earlier invited to an interaction with the Committee for Civil Societies/Academia representatives, on 28.04.2015, though unfortunately, we were unable to attend the same.

Please do let me know if you have any questions or comments.

I look forward to hearing from you.

Yours Sincerely,
For the Internet Democracy Project,

A photograph of a handwritten signature in black ink on a light-colored surface. The signature is written in a cursive style and appears to read 'Nayantara'.

Nayantara Ranganathan,
Programme Manager – Freedom of Expression
Internet Democracy Project

Submission by the Internet Democracy Project

(www.internetdemocracy.in)

**in response to Net Neutrality Department of Telecommunications report, May
2015**

The Department of Telecommunications (DoT) in its report on net neutrality has noted that the Internet is an important public resource and that open and non-discriminatory access to the Internet is crucial to its transformative potential. While the DoT report has affirmed that consumers, civil society, network operators, application providers all have an equal stake in formulating any policy, this insight has not been captured in the ultimate recommendations made, or in the reasoning behind them.

Definitions of net neutrality advanced by the Body of European Regulators of Electronic Communications (BEREC), Prof. Tim Wu and others have been quoted. However, the DoT has expressed “no doubt” that these definitions have to be circumscribed for reasons of having to protect networks from attacks, problems of traffic congestion, need for mechanisms to comply with legal obligations, maintaining a level of quality of service, limitations of bandwidth, data packets having different characteristics etc. This has led to the conclusion that “*the puritan view of net neutrality has practical limitations and does not work in the real world*” [page 14].

What does seem to work in the “real world”, according to the committee, is the business imperative of network operators to have ever-increasing profits. The report has noted that despite the bullish growth in data in recent years, voice continues to be predominant in the telecom space, both in revenues and traffic. The mere *slowing down* of growth in voice revenues in recent years has been a central reason for the committee to erroneously decide that this merits regulation and licensing of over-the-top communication services. It should be emphasized that the communication services over the Internet have provided new and more ways of connecting, and do not really cannibalise the existing traffic over telecom networks for local calls.

Threats to Freedom of Expression

The committee recommends that “*user rights on the Internet need to be ensured so that TSPs/ISPs do not restrict the ability of the user to send, receive, display, use, post any legal content, application or service on the Internet, or restrict any kind of lawful Internet activity or use. The arbiter of what constitutes legality in relation to the content, application or service can only be determined by Government with scope for judicial adjudication in case of any dispute.*”

Freedom of expression has been inadequately addressed and improperly articulated as freedom from content control by TSPs/ISPs. Absence of editorial supervision over the Internet medium is pointed out in the reasoning, while bemoaning the potential for intrusive

control by network operators. However, in the context of the net neutrality debate, this does not sufficiently capture the threats to freedom of expression that traffic management tools and vertical tie-ups bring in the network architecture. Freedom of expression is not safeguarded by merely ensuring that TSPs/ISPs do not restrict user choices in the absolute sense. Restriction should be more broadly understood to include schemes like zero-rating, which incentivise people to use a limited set of applications which are usually up-market oligarchies.

As rightly pointed out in the report, violation of net neutrality brings another layer of negative discrimination to the socially and economically disadvantaged by not offering the whole range of the Internet that fixed broadband users would have access to. Offering a bundle of services at a subsidized price comes at the cost of disincentivising access to other services like independent news websites and websites of social justice movements, which in turn could compromise essential rights like freedom of association.

Interception and monitoring not a net neutrality issue

The Committee has argued that it *“believes that national security is paramount, regardless of treatment of net neutrality. It therefore recommends inter-ministerial consultations to work out measures to ensure compliance of security related requirements from OTT service providers.”*

Interception and monitoring of Internet communications should not be flagged as an issue to be considered under net neutrality debates. The need for interception and monitoring of communications over OTT services has been a rallying point for telecom companies, who argue that the principle of similar treatment of similar services mandates that OTT services be required to provide interception and storing of communications for use by government agencies. Questions have, however, been raised about the constitutionality of such ex-ante interception by the government of telecom networks.¹ In the absence of privacy laws and transparency of legitimacy of requests, extending this existing overreach to online communications would lead to disastrous implications and lead to the chilling of free speech and dissent.

The report claims that in the interest of admirable but diverse goals of national security, public order, decency and morality, protection of privacy, data protection, public safety and disaster communications would be advanced by providing access to communications networks and data regarding communications flow. This means content of communications as well as meta-data. The claim that such conditions “have proved to be extremely valuable in the context of protection of life and property, investigation of criminal offences and preservation of national security” is unfounded and false. In fact, studies² have proven the contrary that there is no reasonable link between mass surveillance of citizens and prevention of terrorism and crime. There is a misguided conflation of protecting the privacy

¹ See <http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights>.

² See https://www.schneier.com/news/archives/2015/06/this_security_expert.html.

of citizens and national security - somehow, the Indian government intercepting communications by requiring servers to be hosted within the country, as opposed to intelligence agencies of other countries accessing our communications, is framed as a privacy win, the absence of strong privacy protections under Indian law notwithstanding.

Network security is ensured through use of secure protocols and a host of other digital hygiene methods. Allowing the government to intercept and store all communications is diagonally opposite to the ostensible goal of network security. Intelligence agencies operating without transparency or checks and balances would be privy to the intercepted information, opening this up to misuse. This stored data is also vulnerable to malicious attacks from third parties. Therefore, it is an altogether different debate that should not be a part of discussions on net neutrality.

No need for level-playing field

The Committee has stated: *"In case of VoIP OTT communication services, there exists a regulatory arbitrage wherein such services also bypass the existing licensing and regulatory regime creating a non-level playing field between TSPs and OTT providers both competing for the same service provision. Public policy response requires that regulatory arbitrage."*

Level-playing field between VoIP OTT communication services and TSPs/ISPs does not come into question. Voice services offered over the Internet cannot be treated the same as those provided by telecom operators. Circuit switching over telecom networks is different from the way packet switching of voice over data works. Further, the imagination of the committee has been limited as to the dynamic nature of application players. For example, WhatsApp was only a messaging service until it recently introduced VoIP. If a license-raj were to be in place, such innovation and changes would also be inhibited.

DoT has not considered that VoIP could be offered by everyone from now-multi-billion dollar companies to independent developers seeking to innovate for socially urgent causes, like women's safety. It is a disservice that the committee looks at the application providers through a commercial lens because a whole gamut of content and applications are developed without commercial motives and this would be inhibited if the barriers to entry and access are increased.

Spectrum limited but optic fibre has more capacity

Another important reasoning of the committee to circumscribe net neutrality is that in the Indian context, over-reliance on mobile as the medium for Internet connectivity has public policy implications. While it is a noble goal of Digital India to envisage access to digital infrastructure as a utility for every citizen, if this does not come with a concomitant equal ease of access to any application or content provider, this would make the Internet less valuable to these Internet users. It would only provide a second-rate service, a limited array of government and industry-backed services, making it not very different from the way

content over television is available. Spectrum licensees should be aware of the evolving nature of technologies and the spectrum limitation problem can be addressed by permissible and transparent traffic management, not by tampering with the agnostic nature of the Internet.

Conclusion

While the report acknowledges that there have been new forms of social interactions, businesses and governance possible through the Internet, due importance to safeguarding the Internet as a destination for public discourse and a site for business innovation has not been given. The repeatedly quoted “core principles of net neutrality” which the committee sees as non-negotiable have not been clearly defined, and the phrase is used more as a proxy for “infrastructure for all”, which is hardly the same thing. Clear formulation of the definition and other nitty-gritties like evaluation criteria and guidelines have been left to TRAI, a body which holds considerations of network operators very dear. If the Internet is to serve the public interest, it is imperative that strong principles to ensure net neutrality are proposed by our policymakers in the government themselves.