

From: kamya@medianama.com

To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>

Sent: Friday, September 1, 2023 10:10:55 AM

Subject: MediaNama's submission to TRAI's consultation paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services

****The authenticity of this message cannot be vouched for. It may be spoofed. Please treat hyperlinks and attachments in this email with caution****

Respected Sir,

Thank you for using a participative approach in discussing the issues of OTT regulation and selective banning of apps. Our submission is a record of the comments that were made at MediaNama's discussion on the regulation and selective banning of OTT communication services.

Comments made by participants at the discussion are quoted/summarised, with paraphrasing for brevity. Please find attached a record of the same.

Regards,

Kamya Pandey

Journalist, MediaNama

App Bans and Network Fees 2023

August 2023

MEDIANAMA

On August 10, MediaNama conducted a live discussion on the regulation and selective banning of calling and messaging platforms, a subject that is currently under consultation by the Telecom Regulatory Authority of India (TRAI). The discussion focused broadly on three themes— the implications of selective banning of applications, the impact of charging calling and messaging platforms a fee for their use of telecom companies' infrastructure, and the creation of a licensing regime for these platforms.

Our objective was to identify:

- How do we define which tech-enabled services get banned during a 'selective' ban?
- Are there technical challenges to banning apps selectively? How do these differ for service providers (the apps/services), the government, etc.?
- Why does TRAI want to venture into selective blocking—when content can be blocked under Section 69A of the IT Act, 2000?
- How will the selective banning of communication services influence the proportionality debate?
- Should apps be required to obtain a license for their operations, just like telecom companies?
- If OTT communication platforms are required to contribute to the Universal Services Obligation Fund (USOF) like telecom companies are supposed to, what would the collected funds be used for?
- What are the implications of charging communication platforms a network fee?
- How do you define communication services and then differentiate a messaging app from a calling app?

Our speakers for the discussion included: Maknoon Wani (Council for Strategic and Defense Research), Samar Bansal (Lawyer), Jhalak Kakkar, (Center for Communication Governance), Amrita Chaudhary (CCAIOI), Neeti Biyani (ISOC), Aman Taneja (Ikigai Law), Sumeysh Srivastava (The Quantum Hub) and Rahil Chatterjee (Ikigai Law).

We saw participation from organisations such as High Court of Delhi, Luthra & Luthra Law, Malayala Manorama, Meta, Outlook, Polygon Technology, PRS Legislative Research, PwC, SAM, Saraf & Partners, Sdela Telecom LLP, Snap Inc, Symbiosis International University, TechCrunch, The Asia Group, The Hindu, The Quantum Hub, United States - India Business Council, USLLS, Viacom18, and Zebra Technologies.

MediaNama hosted this discussion with support from Google and Meta, and in partnership with CCAIOI, the Centre for Communications Governance at the National Law University (Delhi), the Centre for Internet and Society, and The Internet Freedom Foundation.

The following document captures and summarizes the key points raised during the discussion. You can also [view a recording of the discussion](#) on our YouTube channel.

Executive Summary

Almost unanimously, every one of the speakers at MediaNama's discussion on App Bans and Network Fees highlighted that to regulate and selectively ban online communication platforms, one first needs to define what are online communication platforms, or as TRAI calls them, OTT communication apps. Given the diverse services being offered by platforms today, it is hard to decisively conclude what is a communication platform. If platforms where messaging is incidental are excluded from regulation, it would mean that different apps would be subject to varying amounts of regulation. **Moreover, a rigid classification would fail to incorporate future advancements in platforms. So, if a platform that currently only offers messaging and is classified as a “communication app” later decides to offer payments or e-commerce as a function, how would this platform then be classified? That remains unclear.**

The discussion also delved into the confusion around charging communication platforms a network fee for the use of telecom infrastructure. It was mentioned that before deciding on charging network fees, the preliminary focus should be on listing problems that this action would address (if there are any). Further, it was brought up how discussions in India are focused on applying network fees to communications apps in comparison to global discussions covering all those apps that consume a large amount of bandwidth. However, the fact that some major telecom operators are making a significant profit from their businesses, despite claiming that they are losing business because of communication platforms, should be enough to debunk the idea that any online platform should pay a network fee. **Discussants were collectively not in favour of communication platforms being charged a network fee or being asked to contribute to the Universal Service Obligation Fund (USOF). The focus should be on the deployment of the existing USO Fund first, and there is no clear rationale for asking online services to contribute to it. Speakers were of the opinion that network fees could lead to the erasure of net neutrality and could affect people’s access to the internet since the fee would be passed down to the end user.**

Concerning selective banning, discussants said that the internet is largely made up of dominant big tech players, and if these players are shut down, it disrupts critical services.

Moreover, if only these big tech players were banned, bad actors could move on to other lesser-known services. It was agreed that banning orders, be it for specific apps or the internet overall, need to be based on clearly defined and adequately articulated reasons. **Questions were also raised about how federated messaging ecosystems will be managed under the selective banning provisions and that it is also easy for anyone to create an app using XMPP protocols for messaging, and thus, it's impossible to ban a protocol.** It was felt that there was a need for a data-driven assessment of the effectiveness of an internet shutdown before selective app bans are implemented.

Similarly, breaking encryption in lieu of national security was also questioned by the discussants. They said that **end-to-end encryption helps protect people from bad actors and that breaking it would be counterproductive to protecting national security.**

The discussion also reflected on whether communication platforms should be required to obtain a license, just like the telecom companies are currently expected to. It was expressed that this wouldn't be fair, given that for telecom companies, licensing corresponds with exclusivity, which communication apps do not enjoy. Discussants argued that if such a licensing regime was put in place, bigger platforms would be better able to navigate the licensing requirements owing to their considerable resources, and on the same grounds, it remains uncertain whether smaller platforms would be able to ensure compliance or not. Discussants mentioned that regulators must reflect on how licensing might affect consumer choice. **They felt that licensing would create a barrier to entry for newer communication platforms.**

Key Points from the discussion

I. Challenges with defining an OTT communication app

The definition of an OTT communication platform remains unclear:

“While trying to define an app and its primary service, ignore the fact that there is multifunctionality, there is a very wide range of services offered on the same platforms on the same services, and there can be no cookie-cutter approach to this in defining what a messaging service is.” — Neeti Biyani, Internet Society.

Should there even be a specific definition of an app?: Specific categorization of each app/platform fails to incorporate a future advancement of the platform. A platform offering messaging today could also incorporate payments tomorrow, making it tough to allocate it to one category.

IT Rules lack a definition of messaging:

“The IT rules do not define what messaging is. Rule 4.2 says that traceability,... finding the first originator is a requirement only for significant social media intermediaries, primarily in the business of messaging. But in the Twitter section 69A case, the government lawyer argued that when Twitter can't get to the first originator, even though it's mandated under rule 4.2, how can we be expected to reach out to the actual user and issue them the blocking order?” — Aditi Agrawal, Independent Journalist.

What would be addressed through intelligible differentia for calling and messaging services: When it comes to regulation, OTTs are already governed by the Department of Telecommunications, and internet-based services are already governed by the IT Ministry and Ministry of Information and Broadcasting.

The challenge of keeping track of an app's incidental messaging: Platforms that are meant for other purposes, like gaming, can also be used to transmit messages “incidentally” as a part of their services.

“It will be so dynamic, how do you keep track of what is an incidental feature to a service and what is the core functionality also for services that you have been describing that there could be multiple functions that are embedded, right? And one is not in derogation to the other.” — Aman Taneja, Ikigai Law.

Dear Reader,

MediaNama's work of covering the key policy themes that are shaping the future of the Indian Internet is made possible by support from its subscribers. If developments in technology policy are key to you or your organization, I would urge you to [subscribe to MediaNama](#) to support us.

Thanks,
Nikhil Pahwa,
Editor and Publisher

II. Should communication apps be required to obtain a license?

Telecom companies have exclusivity, but the same isn't true for communication apps:

"When they [telecom companies] buy a license, they buy an exclusive license. The license is exclusivity. Every service online does not have exclusivity. They earn their customer base. Telecom operators have an exclusivity where we don't have enough choice. If every app could buy a spectrum and be deployed in this country, I would say sure, let them compete. But every app can't." — Nikhil Pahwa, MediaNama.

Platforms with chatbot integration may also be required to get a license:

"Chatbots today are very popular, as has been mentioned earlier also, across a whole lot of apps, so banking, e-commerce, even government for that matter. Government is also, a whole lot of government services are also, so perhaps when this licensing framework comes, all of those will also require a telecom license, perhaps." — Deepak Maheshwari, Indian Council for Research on International Economic Relations (ICRIER)

Smaller companies may struggle to meet licensing requirements: While bigger companies with the required vast human resources, may be able to navigate a licensing framework even with changes, it is unclear how this framework will affect smaller or home-grown entities. Moreover, if a licensing framework is a means to protect national security, bad actors will just move into unregulated platforms.

The national security argument for licensing:

“The challenge will be if the government uses the national security ground, we have seen courts being hesitant to engage with that and set stuff aside. Though of course, I think there was a Media One judgement sometime back where Chandrachud did try to question the usage of the terminology in national security and saying that the government needs to justify it. So, I mean there are instances where it has been done but we sort of are in this vicious cycle, right now where we come back to national security.” — Jhalak Kakkar, CCG.

How licensing would impact customer choice and market entry:

If licensing of communication platforms is done in the same way that telecom companies are licensed, for a 10-year or 20-year period and where entry and exit are not that difficult, it would reduce the number of platforms available to a customer and would make it difficult for smaller players to enter the communication platform market.

Is the national security argument for licensing proportionate?:

“There is also consequent harm that comes, right? Your ability to speak freely. There is a speech restriction clearly that’s coming in through this sort of national security licensing framework which requires you to share all that information.” — Aman Taneja, Ikigai Law

III. The implications of selectively banning apps

Reasonable objective to ban the Internet: Banning is not always bad, given that Article 19(2) says a “reasonable restriction” is permissible. In the Anuradha Bhasin judgment and others, the court laid down tests of proportionality, and tests of least intrusive methods of imposing a restriction. There must be a “cold-blooded forensic application” of the tests laid down in court judgments to see whether a particular ban is constitutional.

Need for data-driven assessment of internet shutdowns: While there may not be mathematically precise answers, there are other ways to judge the outcome of a ban, which must stand out as a factor in deciding whether a particular approach was effective or not. One such approach can be an analysis of internet shutdowns as well as app bans.

Selective banning of communication apps disrupts critical services, just like an internet shutdown: Selective banning is meant to serve as a mitigative measure against the disruption of critical services like health, education, and finance during a complete internet ban. However, all major communication apps like WhatsApp, Facebook, and Telegram, are “fundamentally integrated” with all these services.

“Let’s take the example of WhatsApp. WhatsApp is used by doctors to consult with specialists. It’s used by students in their classroom groups. Then let’s talk about Telegram. If there are any UPSC aspirants here, you’ll know that all of the content for

UPSC aspirants comes on Telegram. Facebook is used to advertise. It's used to generate leads. My family has a small business. We use WhatsApp, we use Facebook to send samples, photos of samples. So, if you talk about objectives, these apps constitute, let's say more than half of the total internet value chain. If you ban these apps, you're effectively banning a significant portion of the internet. I don't know how these objectives will be met, [and] how this alternative is better than the internet shutdown itself." — Shehlat Makhnoon Wani, Council for Strategic and Defense Research.

Large apps have leverage with the government which can lead to them getting concessions from the government: Because of the centralization of the Internet in the hands of big tech companies, they have certain leverage with the government, and in turn, the government has certain leverage with them.

"..there is going to be an element of negotiation. There is going to be perhaps not a proportionate action against the larger players as they would be against the smaller players. The first point to see is that possibly if at any point of time, there was a ban, let's say, of a larger and more well-used communication, OTT communication app, in terms of the various proportionality and least intrusive principles as laid down by the court that would be far harder for the court, for the government to justify." — Samar Bansal, lawyer.

Bad actors can always migrate to other apps: The use of smaller apps that remain untraceable, unlike WhatsApp or other larger communication platforms.

"bad actors to communicate with each other, perhaps it will have an impact, but probably those bad actors will find a further application that's beyond something the government knows to exchange communication...if you want to get even more targeted, we have to understand what is the implication of maybe shutting down certain actors or nodes within social media platforms. That has serious freedom of speech and expression concerns, but if we are talking about proportionality, I mean, we would even have to start going to that level of granularity." — Jhalak Kakkar, CCG

The act of selective banning is technically challenging:

"So to do this type of blocking [selective blocking at district level], it's not that it is impossible, I mean, you can block something, let's say each and every tower level for that matter, but then that's going to require a huge level of investment by service providers and also much more management from them in terms of technically doing it. So, one [problem] is having the capability, technical capability and feasibility and the other is [the blocking of one particular tower]." — Deepak Maheshwari, Indian Council for Research on International Economic Relations.

Messaging protocols can't be banned: Anyone can use a Jabber XMPP or similar protocol to communicate with any app. So if one app is blocked, those using a messaging protocol can just create another app of their own to communicate on.

The act of selective banning is technically challenging:

“...back in like end of 2000s when Google Talk launched, they were based on a protocol called XMPP, Jabber XMPP and anyone could just take any app and just connect with the protocol like you do an email and you could basically use a Gmail account to chat on that app or on a site anywhere. So how do you ban a protocol? Anyone can set up an app; anyone can use a protocol to communicate with any app; when you move to a federated messaging ecosystem there's no blocking this.” — Nikhil Pahwa, MediaNama

How device-level app-bans are conducted: There are device-level identifiers in banning apps like the roaming setting when a person travels from Delhi to Jaipur. This is done by referring to companies' Home Location Registry (HLR) and Visitor Location Registry (VLR).

Selective app bans require people's devices to be tracked, which can be a major privacy concern:

“... [if] an app needs to be kind of selectively banned in a particular area, the telecom provider has to have [always an] access to the device so that they can track it and switch it off. So I, as a user, have to give that access. And if someone is kind of getting into my system and accessing it without my consent, that is a privacy concern,” —Amrita Choudhury, CCAOI

Section 69A of the IT Act has no unblocking mechanism: A blocking order for apps can only be rolled back if the review committee disagrees with it.

Banning orders need to be specific in nature:

“Every decision of the government has to be on the basis of some material so that ultimately they say that reasons are the lifeblood of every order. So therefore, someone reading, assessing, and wanting to challenge [the order] must know why it was there.” — Samar Bansal, lawyer.

Need for transparency in Internet shutdowns: The parliamentary standing committee had suggested that there was a need to create a database of shutdowns and to actually review those shutdowns.

“So we're now talking very specifically and we're kind of shifting the goalpost here when the core of the issue remains and someone has a brilliant point about national security, important, very important to consider, but where is accountability and transparency in the executive action and that somehow I feel like this entire

conversation is shifting the core issue that needs to be re-emphasized continuously. We don't have data on internet shutdowns officially in the country. Now we're coming in with app ban shutdowns. What's going to happen there? Are you just empowering an executive to build on the various actions already taken?" — Rahil Chatterjee, Ikigai Law

IV. Should communication apps be charged for their use of telecom infrastructure?

Telecom business model has changed: The crux of the argument behind network fees is that communication platforms offer the same services as telecom companies (calling and messaging) and are eating away at telecom companies' customer base, even though the telecom business model has changed completely because of the transition to data.

"If you look at it today, my Vodafone telco does not charge me for SMSes or voice. They are earning from me from data. So, this is their business strategy - they will earn money from data. If their voice revenue or SMS revenue is decreasing, that's because they are not charging me that way. They know where the money comes from," — Amrita Choudhury, CCAOI.

Telecom companies must be expected to invest in their own infrastructure: According to a study conducted by TMT management consulting firm Analysys Mason in Europe, between 2018 and 2021, when telcos made an [network-related ISP] investment of 3%, the network traffic increased by 160%.

The European regulator is not in favor of a network fee: The TRAI consultation refers to a report by the Body of European Regulators for Electronic Communications (BEREC) report which refutes the need for network fees. Further, there is a question of why network fees should only be charged to communication platforms.

Global network fee discussions are focused on traffic and not the nature of the service (communications):

"If you actually look at what network usage fees is related to, specifically across the globe, when you look at any sort of other conversations, it's about traffic generation," — Rahil Chatterjee, Ikigai Law.

OTTs are responsible for quality of service even after paying a network fee in South Korea: In 2021-22, South Korea said that all online platforms have to pay a certain fee to move their traffic through a telecom company's network.

“The concerning part out there is that even after paying, the OTT is responsible for the quality of services, it goes to the customer. And, what they ultimately did is, an ISP can say that they will not take, not carry the data of a particular service provider if they do not pay. Does India want to go to that scenario?” — Amrita Choudhury, CCAOI.

Need for an assessment of what the network fee’s purpose is: In the US, a bill is currently being tabled to decide whether there is a need for a revenue share agreement between telecom companies and online platforms. This bill is conducting a primary assessment of the problem network fees solve, a similar assessment is needed in India as well.

Network fees would lead to a rise in the cost of online services for the end user: If a network fee arrangement is implemented, eventually, the end user will have to incur the fee. This is a concern especially because internet penetration in India is now shifting from urban centers to rural areas.

“Imagine increasing the cost of services in rural areas. You’re not going to have the same buy-in on the internet and the entire digital ecosystem.” — Rahil Chatterjee, Ikigai Law.

Should OTT Companies be required to contribute to the USO Fund?

No rationale for asking OTT companies to pay: Licensing brings exclusivity, for which telecom companies may be asked to pay for the USO Fund in order to assist in telecom infrastructure deployment. OTT Companies operate in an environment of infinite competition and have no exclusivity.

USO Fund is under-utilised. First that should be deployed

“You have a USO (Universal Services Obligation) fund lying, which the telecom operators are paying. What is happening to it? Should it not be used when infrastructure has to be made, or should it only be given to [the] power grid or RailTel [a public sector enterprise that provides broadband services]? Why can it not be given to the others who are building infrastructure? Why is that money not utilized when telcos are suffering?” — Amrita Choudhury, CCAOI.

How Competition encourages telecom companies to create better infrastructure:

“I’m a great believer in competition. Competition builds infrastructure. If you go back to when Jio launched and just six months before Jio launched, Airtel started an initiative called the One Network Initiative. At that point in time, they started

improving their infrastructure at breakneck speeds to the extent that Airtel infrastructure everywhere across the country improved drastically. Why? Because they were afraid of Jio, right?” — Nikhil Pahwa, MediaNama

V. Why end-to-end encryption on communication apps needs to be preserved

End-to-end encryption should be preserved to keep people safe online: While it might be said that end-to-end encryption leads to national security issues, it also provides people with the digital equivalent of having a conversation in a closed room.

“So, E2E encryption is not a law enforcement issue alone. It is a technology that helps keep a lot of people extremely safe, including children, the elderly, women, marginalised populations. So, when you talk about proportionality, I want to approach this issue beginning from there. Are we not willing to take into account the concerns that the most downtrodden, underprivileged, marginalised people in our country have? Do they have that right to be a citizen, not a subject?” — Neeti Biyani, Internet Society.

Breaking encryption does not help national security: While national security as grounds for interception may not pass the proportionality tests, there have been instances like the Pegasus case where courts tend to give in to this argument. Rather than solely focusing on the grounds, it should be argued that breaking encryption encourages more bad actors.

“[We should argue] you are creating more and more risks for people who are on the internet. It might not work from the point of view of national security but you are not really helping to create a safer internet experience for people.” — Sumeysh Srivastava, The Quantum Hub.

Law enforcement agencies working at the grassroots level lack technical assistance:

“...where [law enforcement agencies] need access to some sort of data which is located elsewhere and at times because the parent organization or the data centers are located outside, it becomes extremely difficult for these enforcement agencies to get hold of that data. The issue also lies with the lack of capacity building and technical assistance. Most of the times our legal enforcement agencies, the one who work at the very grassroot level, they don't really have a very clear idea of how to transmit these requests and what all should form part of this.” – Sukanya Thapliyal, CCG-NLUD

Companies and enterprises are slapped with personal criminal liabilities:

“...[what] we're seeing in regulation increasingly is that there's a personal criminal liability aspect that seems to come in repeatedly for enterprises and companies. It's happened in social media and the IT rules as well. Why do you have a situation of personal criminal liability in law? And this is something that needs to be addressed in the Digital India Act...founders are complaining about the fact that most of these are unicorn founders. So, they're like, this state, this place, this case has been filed, a criminal case has been filed, and my name is there. So, at some level at police stations, the FIRs are just naming, like you've got criminal FIRs sort of being filed against founders on one level. But even in law itself, you've seen this change where there's personal criminal liability for employees of the company.” – Nikhil Pahwa, MediaNama

Reference Material

- What Are The Technical And Regulatory Challenges In The Selective Banning Of Online Apps? [[Read](#)]
- App Bans Over Internet Shutdowns? Experts Explore Issues Around Effectiveness, Impact, And Transparency [[Read](#)]
- Do We Need Specific Definitions Of Services To Regulate OTT Apps? [[Read](#)]
- Is It Fair To Charge Communication Platforms A Network Fee? [[Read](#)]
- Should Communication Apps Contribute To The USO Fund? [[Read](#)]

Additional Reading

On Regulating OTT communication platforms:

- [A Summary: TRAI Releases Consultation Paper On Calling And Messaging App Regulation](#)
- [Reliance Jio Wants Regulation for All Internet Co's in India, Hosting in India – TRAI OTT Consultation.](#)
- [Ashwini Vaishnaw On Draft Telecom Bill Regulating WhatsApp, Mandating KYC And Revealing Caller Identity](#)
- [COAI Seeks Regulation Of 'Communication OTTs', Not All OTTs: S P Kochhar on the Draft Telecom Bill](#)
- [The Internet Freedom Foundation's concerns with how the Telecom Bill, 2022, approaches OTT regulation, through 'straitjacketing' diverse Internet platforms.](#)
- [Ten recommendations on the draft Telecom Bill, 2022: SFLC](#)
- [How The Telecom Bill 2022 Undermines The Potential of Internet: Internet Society's Report](#)
- [Want Telco-Like Regulation For OTTs: Jio's Submission to DoT ahead of draft telecom bill](#)
- [Reliance Jio Shares Thoughts On The Draft Telecom Bill, And They're Worth Noting!](#)
- [Raising surveillance concerns, India's draft Telecom Bill 2022 proposes allowing the government to intercept messages or suspend the Internet during public emergencies, if "necessary" or "expedient".](#)
- [AIC Says No To 'Same Service, Same Rules' In Comments On The Telecom Bill 2022 Draft telecommunication bill asks for KYC on platforms like Whatsapp and Zoom.](#)

Historical context of OTT regulation:

- [#NetNeutrality: TRAI Rules That Differential Pricing Will Not Be Allowed](#)
- [Either Regulate WhatsApp Like OTTs Or Relax Telcos' Regulatory Burden, Says COAI](#)

- [Live \[Closed\]: TRAI Open House Discussion on OTT Regulation – Delhi](#)
- [TRAJ’s net neutrality open house discussion on traffic management practices in 2020](#)
- [MediaNama’s comments to TRAI on traffic management and an advisory body for Net Neutrality](#)

On network fees:

- [European Union’s Proposal To Get Big Tech To Pay Interconnection Fee Threatens Net Neutrality](#)
- [South Korean Internet Service Provider Sues Netflix, Reigniting Debate On Net Neutrality](#)
- [How bad policy led South Korea into a Net Neutrality nightmare](#)
- [A Shared And Open Internet Vs. ‘Exclusive Gardens’: Imposing ‘Network Costs’ On OTTs A Bad Idea?](#)
- [Six Talking Points From The EU’s Exploratory Consultation On OTT Players Sharing Investment Costs With Telcos](#)

On internet shutdowns:

- [Manipur High Court recommends partial lifting of internet ban and providing internet services through restricted channels and “whitelisted” numbers.](#)
- [A Parliamentary panel report on cybersecurity proposes a whitelisting framework for lending apps.](#)
- [The Centre for Internet and Society’s Co-Founder Pranesh Prakash explains the various issues with how Section 69A orders are being executed in India currently. India tops the list of most Internet shutdowns for the fifth year running, with 84 in 2022.](#)
- [Parliamentary Standing Committee on Communications and Information Technology criticises the Indian government for lack of data on Internet shutdowns, and for lack of review processes on shutdowns.](#)
- [The Internet Freedom Foundation and Human Rights Watch release a report detailing the human impact of Internet shutdowns in India, titled “No Internet Means No Work, No Pay, No Food”.](#)
- [Calcutta High Court rules that the West Bengal government did not follow the correct procedures while ordering shutdowns in the state last year. Panelists at a MediaNama event question whether Indian courts are doing enough to question state intrusions on fundamental rights, like accessing the Internet.](#)
- [Report: A closer look at India’s website blocking practices and everything that’s wrong with it.](#)

[Airtel uses specially configured routers to block websites: Why you should care.](#)

MediaNama's previous discussions on OTT regulation:

- [How Will A Licensing Regime For Online Services In Convergence Framework Create Barriers To Entry? #NAMA](#)
- [No clarity on aspects that a converged regulator will focus on: Expert on TRAI's Convergence Paper #NAMA](#)
- [Will Self-Regulation By Streaming Platforms Help Curb Harmful Content? #NAMA](#)
- [Is India's Telecom Regulator Equipped To Deal With Issues Related To Quality Of Services? #NAMA](#)

MediaNama is the premier source of information & analysis on Digital Policy in India. We focus on key issues like privacy, data governance, fake news, misinformation, cybersecurity, cyber diplomacy, digital payments policy, Net Neutrality, intermediary liability, website blocking, internet shutdowns, data localisation, e-commerce policy, IoT, content regulation and censorship, among others.

Our mission is to help build a digital ecosystem which is open, fair, competitive, and global.

On MediaNama.com, our reportage attracts a readership of policy professionals, government officials, Members of Parliament, startup founders and business leaders, as well as investors with an eye on policy developments shaping the future of the Internet in India.

MediaNama's events enable meaningful conversations for a high quality and curated audience to discuss opportunities, challenges and issues that they care about, in a manner that helps in building capacity. The fact that they are among peers with similar depth of understanding, and come at the same issues from a different point of view, ensures that our audience keeps coming back for more.

Nikhil Pahwa | Founder & Editor | nikhil@medianama.com

MediaNama.com | [Twitter](#) | [Facebook](#) | [YouTube](#) | [LinkedIn](#)
Subscribe to [Telegram](#) | [Newsletter](#)