LEXMENTOR

Legal Research and Policy Advisory

New Delhi, India | contact.lexmentor@gmail.com

PUBLIC CONSULTATION SUBMISSION

Comments and Suggestions on the Consultation Paper on the

'Proliferation of Public Wi-Fi Networks in India'

Telecom Regulatory Authority of India -- Division of Broadband and Policy Analysis

Addressed To	Dr. Abdul Kayum, Advisor (Broadband and Policy Analysis), Telecom Regulatory Authority of India, New Delhi
Via	advbbpa@trai.gov.in with copy to jtadvbbpa-1@trai.gov.in
Reference	Consultation Paper No. 54 of 2026, dated April 27, 2026
Deadline	May 25, 2026 (Comments); June 8, 2026 (Counter-Comments)
Prepared By	Aditya Sharma, Academic Head, LexMentor Aaditya Wadhwa, Academic Research Fellow, LexMentor
Submitted By	LexMentor Legal Research and Policy Advisory, New Delhi

Prefatory Note: *LexMentor Legal Research and Policy Advisory is a legal research and policy engagement platform based in New Delhi, India, committed to advancing evidence-based scholarship on constitutional law, telecommunications regulation, digital rights, and technology policy. We welcome TRAI's initiative in releasing the Consultation Paper on the Proliferation of Public Wi-Fi Networks in India and commend the Authority for undertaking a comprehensive review of the existing regulatory framework. The following submissions are offered from the perspective of constitutional law, digital rights, and the imperative of equitable access to digital infrastructure for all citizens of India, including those in rural, remote, and underserved communities.*

I. Background -- Public Wi-Fi as a Constitutional and Policy Imperative

Access to the internet is no longer a luxury or a matter of commercial convenience -- it is an essential precondition for the meaningful exercise of fundamental rights guaranteed under the Constitution of India. The Supreme Court of India, in Anuradha Bhasin v. Union of India (2020), recognised the freedom to practice any profession or carry on any occupation, trade, or business over the internet as a fundamental right under Article 19(1)(g), and the freedom of speech and expression through internet media as protected under Article 19(1)(a). Public Wi-Fi infrastructure is the most direct mechanism through which the State can operationalise these rights for citizens who lack the means to access private broadband connections.1

India's public Wi-Fi ecosystem has seen significant policy attention since the launch of the PM-WANI (Prime Minister Wi-Fi Access Network Interface) scheme in December 2020, which created a decentralised framework for the deployment of public Wi-Fi hotspots through Public Data Offices (PDOs), Public Data Office Aggregators (PDOAs), and App Providers. Despite these efforts, the growth of PM-WANI deployments has fallen significantly short of aspirational targets, with key challenges including low commercial viability, inadequate roaming infrastructure, complex authentication requirements, and insufficient participation by local bodies and state governments.2

TRAI's Consultation Paper No. 54 of 2026, dated April 27, 2026, is therefore both timely and important. LexMentor's submissions address the constitutional and rights-based dimensions of public Wi-Fi governance; the regulatory and authorisation framework for PDOs and PDOAs; authentication, roaming, and billing architecture; rural and underserved area deployment; data protection and user privacy; and revenue and sustainability models appropriate to the Indian context.

II. Constitutional Framework -- Right to Internet Access and Public Wi-Fi

Observation: The constitutional recognition of internet access as a fundamental right in Anuradha Bhasin creates a positive obligation on the State to progressively realise equitable internet access for all citizens. Public Wi-Fi infrastructure -- particularly in rural areas, peri-urban communities, and among economically marginalised populations -- is the primary mechanism through which this positive obligation can be discharged for citizens who cannot afford or do not have access to private broadband. The current regulatory framework for public Wi-Fi does not adequately reflect this constitutional dimension.3

Suggestions:

- TRAI should recommend that the Government of India formally recognise public Wi-Fi access as a component of the right to digital inclusion, and incorporate a minimum public Wi-Fi coverage standard into the Universal Service Obligation Fund (USOF) framework, with dedicated funding for deployment in districts with below-average internet penetration rates.
- A constitutional impact assessment should be conducted before any restriction is imposed on public Wi-Fi access -- including geographic restrictions, bandwidth caps, or authentication requirements -- to ensure that such restrictions satisfy the tests of legality, necessity, and proportionality under Articles 19(2) and 19(6) of the Constitution.
- Public Wi-Fi infrastructure in government buildings, public transport hubs, panchayat offices, primary health centres, and government schools should be mandated as a minimum standard of public service delivery, with implementation responsibility assigned jointly to DoT, MeitY, and the relevant line ministries.

III. PM-WANI Framework -- Assessment and Recommendations

Observation: The PM-WANI scheme, launched in December 2020 with the objective of creating a decentralised, licence-free ecosystem for public Wi-Fi deployment, was a bold and well-conceived policy initiative. However, five years after its launch, the scheme has not achieved its intended scale. Key structural weaknesses include the absence of a commercially viable revenue model for PDOs, the lack of seamless roaming between networks of different PDOAs, the complexity of the registration-based authentication requirement, and the limited awareness and capacity of potential PDOs -- particularly small shopkeepers and local entrepreneurs -- to navigate the PDOA onboarding process.4

Suggestions:

- TRAI should recommend a comprehensive review and simplification of the PM-WANI registration and onboarding process for PDOs, with a target of reducing the time from application to deployment to no more than 48 hours. A single-window online portal, supported by a dedicated helpline in regional languages, should be established for PM-WANI registrations.
- The PDOA framework should be restructured to enable larger aggregators -- including telecom service providers, state government agencies, and established ISPs -- to onboard PDOs at scale under a simplified master agreement, reducing the per-PDO administrative burden that currently deters participation.

- A minimum guaranteed revenue model for PM-WANI PDOs should be designed, potentially through a USOF-backed viability gap funding mechanism, to ensure that deployment in low-footfall or low-income areas is commercially sustainable even in the absence of advertising or premium service revenues.
- TRAI should recommend the adoption of the Passpoint (Hotspot 2.0) standard for PM-WANI networks to enable seamless, automatic roaming across different PDOA networks without requiring repeated manual authentication by users -- one of the most significant barriers to the user experience of public Wi-Fi in India.

IV. Authentication, Roaming, and Billing Architecture

Observation: The current authentication framework for public Wi-Fi in India -- which requires OTP-based verification linked to a mobile number at every new network -- is simultaneously a security requirement and a major usability barrier. International experience demonstrates that frictionless, seamless authentication through standards such as Passpoint, OpenRoaming, and carrier-grade Wi-Fi offload significantly increases public Wi-Fi adoption and usage, without compromising the ability of law enforcement to obtain lawful access to user records when required.5

Suggestions:

- TRAI should recommend the adoption of a tiered authentication framework: mandatory OTP-based authentication for first-time registration, followed by automatic re-authentication for returning users through device-based credentials or SIM-based authentication, eliminating the need for repeated OTP entry at each session.
- A national public Wi-Fi roaming framework -- modelled on the Wireless Broadband Alliance's OpenRoaming standard -- should be developed under TRAI's oversight, enabling seamless roaming between PM-WANI, TSP-operated, and municipal Wi-Fi networks through a common identity and policy framework.
- The billing and settlement architecture for inter-PDOA roaming should be standardised by TRAI through a prescribed settlement framework, preventing the commercial fragmentation that currently makes multi-network roaming commercially unviable for PDOs.
- For public Wi-Fi deployed in government premises and public spaces with USOF funding, authentication requirements should be reduced to device-based registration only -- without mandatory mobile number linkage -- to protect the privacy of users who do not wish to be

identified, consistent with the right to informational privacy under Article 21 of the Constitution.

V. Rural and Underserved Area Deployment

Observation: The digital divide between urban and rural India remains one of the most significant structural inequalities in the country. While urban India has seen rapid growth in both private broadband and public Wi-Fi availability, rural India -- where more than 65% of India's population lives -- continues to have severely limited access to high-quality internet connectivity. The Consultation Paper's focus on rural deployment is therefore one of the most important dimensions of this exercise, and LexMentor strongly urges TRAI to place the rural digital divide at the centre of its recommendations.

Suggestions:

- TRAI should recommend a Rural Public Wi-Fi Mission -- distinct from PM-WANI's urban-oriented framework -- with specific targets for the number of public Wi-Fi hotspots per gram panchayat, dedicated USOF funding, and implementation responsibility assigned to the Common Service Centre (CSC) network and state e-governance agencies.
- The BharatNet fibre network, which now connects a significant proportion of gram panchayats, should be mandatorily leveraged to provide backhaul connectivity for rural public Wi-Fi hotspots, with TRAI recommending a minimum backhaul bandwidth standard of 100 Mbps per hotspot to ensure adequate quality of service.
- State governments should be required, as a condition of USOF disbursements, to integrate public Wi-Fi deployment into their district digital infrastructure plans, with specific coverage targets for primary health centres, agricultural market yards (mandis), gram panchayat offices, and government schools.
- A digital literacy and awareness programme should be coupled with every rural public Wi-Fi deployment, to ensure that the infrastructure is actually used by the communities it serves, particularly women, elderly persons, and first-generation internet users.

VI. Data Protection, User Privacy, and Cybersecurity

Observation: Public Wi-Fi networks present distinctive data protection and cybersecurity challenges. Users of public Wi-Fi are typically on shared, unencrypted or weakly encrypted networks, creating significant risks of traffic interception, man-in-the-middle attacks, and unauthorised access to personal data. At the same time, the mandatory collection and retention of user authentication data for law enforcement purposes creates a significant store of personal data that, if inadequately secured, poses serious privacy risks. The Digital Personal Data Protection Act, 2023 (DPDP Act), and the forthcoming DPDP Rules impose specific obligations on data fiduciaries that PDOs and PDOAs must comply with, and TRAI's recommendations must be aligned with this framework.

Suggestions:

- TRAI should prescribe mandatory minimum cybersecurity standards for public Wi-Fi networks, including WPA3 encryption as the minimum standard for all new deployments, network isolation between user sessions, and regular security audits for PDOAs with more than 100 active hotspots.
- A clear data retention framework for public Wi-Fi authentication logs must be prescribed, specifying the maximum retention period (recommended: 90 days), the security standards for storage, and the conditions for disclosure to law enforcement agencies, consistent with the DPDP Act, 2023, and the Supreme Court's right to privacy jurisprudence in K.S. Puttaswamy v. Union of India.
- PDOs and PDOAs should be classified as 'Data Fiduciaries' under the DPDP Act, 2023, and should be required to publish a clear, accessible privacy notice to users at the point of authentication, disclosing the data collected, the retention period, and the conditions of disclosure to third parties.
- A user opt-out mechanism for non-essential data collection -- including location tracking, browsing history, and device fingerprinting -- should be mandated for all public Wi-Fi networks, with non-essential data collection prohibited entirely for USOF-funded deployments.

VII. Stakeholder Roles -- Government, Local Bodies, TSPs, and Private Entities

Observation: The Consultation Paper correctly identifies the multiplicity of stakeholders involved in public Wi-Fi deployment -- Central Government, State Governments, Urban Local Bodies (ULBs), Panchayati Raj Institutions (PRIs), Telecom Service Providers (TSPs), ISPs, and private entities -- as both a strength and a governance challenge. The current framework does not clearly assign

responsibility for deployment in different categories of locations, leading to gaps in coverage and duplication of effort in commercially attractive locations.

Suggestions:

- TRAI should recommend a clear jurisdictional framework for public Wi-Fi deployment, assigning primary responsibility as follows: Central Government agencies for national transport hubs, central government offices, and central educational institutions; State Governments for state government offices, district hospitals, state highways, and state-run transport terminals; ULBs for urban parks, markets, and public spaces; and PRIs for gram panchayat offices and rural public spaces.
- Urban Local Bodies should be required to include public Wi-Fi infrastructure in their Smart Cities Mission and AMRUT 2.0 plans, with TRAI recommending minimum coverage standards for cities above a prescribed population threshold.
- A Public-Private Partnership (PPP) framework specifically designed for public Wi-Fi deployment -- with a model concession agreement, revenue sharing norms, and performance benchmarks -- should be developed by TRAI in consultation with the Ministry of Finance and the Department of Telecommunications, to attract private investment into commercially marginal but socially important deployment locations.

VIII. Revenue Models and Commercial Sustainability

Observation: The commercial sustainability of public Wi-Fi deployment -- particularly in rural and semi-urban areas -- is the central challenge that the current framework has failed to adequately address. PDOs operating under PM-WANI have found it difficult to generate sufficient revenue from Wi-Fi services alone, given the prevalence of cheap mobile data plans in India. A sustainable revenue model must therefore combine multiple revenue streams and public funding support to make deployment viable across diverse economic contexts.

Suggestions:

- TRAI should recommend a hybrid revenue model for public Wi-Fi that combines: tiered free and paid access (with a minimum free tier of 30 minutes per day per user at no charge, funded through USOF or municipal budgets); local advertising revenues for hotspots in high-footfall

commercial locations; and premium quality-of-service tiers for users requiring higher bandwidth.

- A voucher-based access model -- enabling government welfare programme beneficiaries, students, and senior citizens to access public Wi-Fi free of charge through their Jan Dhan or Aadhaar-linked accounts -- should be piloted by TRAI in partnership with MeitY and the Ministry of Finance.
- Wi-Fi offload agreements between TSPs and PDOAs should be facilitated through a standard commercial framework prescribed by TRAI, enabling TSPs to route mobile data traffic through public Wi-Fi networks in exchange for a revenue share with PDOAs -- creating a sustainable indirect revenue stream that does not depend on end-user payments.
- The USOF should be restructured to provide both capital expenditure grants (for hardware and installation) and operational expenditure support (for backhaul, power, and maintenance costs) for public Wi-Fi in underserved areas, with performance-linked disbursement tied to uptime, user adoption, and data usage metrics.

IX. Issue-Specific Recommendations -- Summary Table

The following issue-specific recommendations are respectfully submitted for TRAI's consideration:

Issue Area	Observation	Recommendation
PM-WANI PDO Onboarding	Complex onboarding process deters potential PDOs, particularly small entrepreneurs in rural areas.	Simplify to a 48-hour single-window online process with regional language support and a dedicated helpline.
Authentication Framework	Repeated OTP requirements at every new network create significant usability friction and depress public Wi-Fi adoption.	Adopt tiered authentication: one-time OTP registration, followed by automatic device-based re-authentication for returning users.
Roaming Architecture	Absence of inter-PDOA roaming means users must re-authenticate at every network, defeating the purpose of seamless public Wi-Fi.	Adopt Passpoint/OpenRoaming standards and prescribe a mandatory inter-PDOA settlement framework.
Rural Deployment	PM-WANI's urban-centric design has failed to address the rural digital divide, with inadequate deployment in gram panchayats and primary health centres.	Launch a dedicated Rural Public Wi-Fi Mission with USOF funding, BharatNet backhaul mandates, and CSC network implementation.

Data Protection and Privacy	No minimum cybersecurity standards or data retention limits are prescribed for public Wi-Fi networks, creating privacy risks for users.	Mandate WPA3 encryption, 90-day maximum log retention, DPDP Act compliance, and user opt-out for non-essential data collection.
Revenue Sustainability	The current framework lacks a viable revenue model for PDOs in low-footfall or low-income areas, causing deployment gaps.	Prescribe a hybrid model combining a USOF-funded free tier, local advertising, TSP Wi-Fi offload agreements, and welfare voucher access.

X. Conclusion

LexMentor commends TRAI for releasing this Consultation Paper at a critical juncture in India's digital infrastructure journey. Public Wi-Fi is not merely a telecommunications policy question -- it is a constitutional imperative, a social equity instrument, and a foundation for India's digital economy. The gap between aspirational targets and ground-level deployment under PM-WANI demonstrates that technical and commercial solutions alone are insufficient without a clear rights-based framework, equitable funding mechanisms, and genuine accountability for deployment outcomes.

The recommendations set out in this submission are offered constructively, with a view to ensuring that TRAI's final recommendations to the Government are ambitious, constitutionally grounded, and operationally workable across the full diversity of India's geography, economy, and society. LexMentor remains available for any further engagement, clarification, or participation in any stakeholder consultation that TRAI may organise, and respectfully reserves the right to submit counter-comments on the responses of other stakeholders by June 8, 2026.

Respectfully submitted,

LexMentor Legal Research and Policy Advisory

Aditya Sharma | *Academic Head*

Aaditya Wadhwa | *Academic Research Fellow*

New Delhi | *contact.lexmentor@gmail.com*

Footnotes and References

1. *Supreme Court of India, Anuradha Bhasin v. Union of India, (2020) 3 SCC 637. The Court held that freedom of speech and expression and freedom to practice any profession or carry on any occupation, trade, or business over the internet is protected under Articles 19(1)(a) and 19(1)(g) of the Constitution of India.*
2. *TRAI, Consultation Paper on the 'Proliferation of Public Wi-Fi Networks in India', Consultation Paper No. 54 of 2026, April 27, 2026. Available at: trai.gov.in. Written comments invited by May 25, 2026; counter-comments by June 8, 2026.*
3. *PIB, 'TRAI Releases Consultation Paper on Proliferation of Public Wi-Fi Networks in India', Press Release dated April 27, 2026. Available at: pib.gov.in. The Consultation Paper covers authorisation, authentication, roaming, billing, stakeholder roles, and revenue models for public Wi-Fi.*
4. *Medianama, 'TRAI releases consultation paper on public Wi-Fi deployment' (April 27, 2026). Available at: medianama.com. The paper highlights low PM-WANI deployments and proposes Passpoint, roaming, and funding reforms to scale India's public Wi-Fi infrastructure.*
5. *Wireless Broadband Alliance, 'OpenRoaming: The Global Wi-Fi Roaming Framework' (2023). The OpenRoaming standard enables automatic, secure Wi-Fi roaming across participating networks globally, removing the need for per-network authentication and providing a user experience comparable to cellular roaming.*
6. *Supreme Court of India, Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. The nine-judge bench unanimously recognised the right to privacy as a fundamental right under Article 21 of the Constitution, with implications for the collection, retention, and use of personal data by public Wi-Fi operators and government agencies.*
7. *Digital Personal Data Protection Act, 2023 (No. 22 of 2023). PDOs and PDOAs collecting authentication data from users of public Wi-Fi networks are 'Data Fiduciaries' within the meaning of Section 2(i) of the Act and are subject to its provisions regarding consent, data minimisation, purpose limitation, storage limitation, and data security.*

-- End of Submission --