Response to TRAI Consultation Paper No. 07/2026 on Proliferation of Public Wi-Fi Networks in India

jtadvbbpa-1 < jtadvbbpa-1@trai.gov.in >

< aditya.chaudhuri@advayanet.ai >

Thu, 21 May 2026 10:02:33 AM +0530

To "advbbpa"<advbbpa@trai.gov.in>

Cc "jtadvbbpa-1"<jtadvbbpa-1@trai.gov.in>

Tags Not in Contacts

Submitted by: Advaya Networks Pvt. Ltd.
Authored by: Aditya Chaudhuri, Founder & CTO
Date: 21 May 2026
Kind Attn: **Dr Abdul Kayum, Advisor (BB&PA), TRA**I · advbbpa@trai.gov.in · cc: jtadvbbpa-1@trai.gov.in

About the respondent
Advaya Networks is an AI-native RAN optimisation deep-tech company headquartered in Gurugram, working at the intersection of 5G/6G radio access, edge inference, and operator-grade network analytics. We are a member of the NVIDIA Inception programme and a registered Ericsson EIAP rApp developer. The undersigned has 38 years of telecom industry experience across operator, OEM, and standards roles, is a Senior Member of IEEE, a Fellow of IETE and IE(I), serves on the ACM India Technology Policy Committee, and is a Professor of Practice at IIT Mandi (SCEE). Our perspective on this consultation comes from the operator-engineering and standards-developer side of the ecosystem.

We thank TRAI for inviting public comment on a paper that is unusually thorough in its diagnosis. The consultation document has effectively done the hard work of cataloguing what is wrong with PM-WANI economics and what international practice would recommend; the harder question is what India should now actually do? That is what we attempt to address below. We restrict our response to nine questions where Advaya has direct operator-engineering authority. On the remaining seventeen, we defer to stakeholders better placed to comment.

Q1. Supply-side constraints affecting Public Wi-Fi proliferation
The paper's own paragraphs 2.85 through 2.93 are accurate, and we endorse the diagnosis. We would add three constraints that the discussion underweights.

1. **First, the wholesale bandwidth pricing regime for PDOs is opaque**. The Tariff Order 71st Amendment (2025) caps FTTH for PDOs at twice the equivalent retail tariff (para 2.60), but there is no public mechanism to verify compliance, no published reference price for backhaul bandwidth supplied to PDOAs, and no recourse where a PDO cannot obtain bandwidth at the capped price. The cap is well-intentioned, but unenforced caps are commercial fiction.
2. **Second, the power tariff treatment for outdoor hotspots sits in regulatory limbo.** Streetlight-mounted access points draw a few watts continuously, but municipal electricity tariffs are not structured for telecom infrastructure consumption

on shared assets. Aggregated billing across multiple units, as the paper itself notes in para 2.98, is the technically obvious answer and remains administratively absent.
3. **Third, and most importantly for the longer arc, India has no mechanism to ensure that PM-WANI hardware specifications keep pace with the evolution of Wi-Fi standards.** Wi-Fi 6E and Wi-Fi 7 (802.11be) are now in mature commercial deployment globally, and the paper rightly notes the December 2024 notification on 6 GHz delicensing and the December 2025 TRAI recommendations on V-band (paras 2.62 and 2.66). But PDO-grade equipment in the field remains predominantly Wi-Fi 5- or early Wi-Fi 6-capable, and the PM-WANI framework provides no mechanism to tie future Digital Bharat Nidhi-funded deployments to a minimum generation standard. **A subsidy that funds yesterday's hardware is one the market will need to fund again in three years.**

Recommended measure: *Mandate that any PM-WANI deployment receiving direct or indirect public funding (DBN, SASCI-linked state grants, Smart City budgets) must use Wi-Fi 6E-or-newer access points, with a defined sunset for legacy hardware. Publish a quarterly reference price for FTTH backhaul supplied to registered PDOs, and create a grievance route where PDOs can flag non-compliance with the 2× cap.*

Q4. Changes to the PM-WANI framework for revenue certainty and sustainability of PDOs/PDOAs

PM-WANI's revenue problem is structural, not regulatory. Paragraph 2.88 of the consultation paper sets it out plainly: when users are unwilling to break their mobile data session for the small marginal saving on Wi-Fi vouchers, each hotspot serves a small number of paying customers per day, and per-hotspot ARPU does not cover backhaul, electricity, and equipment costs. **The framework cannot make users pay; it has to find revenue elsewhere.**

Three changes would materially improve the position.

1. **The first is to legitimise and standardise indirect revenue streams.** Today, the PM-WANI architecture is silent on whether a PDOA can monetise anonymised footfall analytics, sell location-aware advertising on the captive portal, or bundle Wi-Fi access into B2B propositions with venue owners. This silence creates legal uncertainty and discourages innovation. A clear, positive list of permitted monetisation models, with corresponding consent, anonymisation, and data-handling obligations, would unlock revenue without further user friction.
2. **The second is to explicitly enable PDOA-to-PDOA settlement so that inter-hotspot roaming (addressed in Q24) becomes commercially viable.** Without a settlement mechanism, a PDOA carrying another's users has every incentive to make the experience worse, not better. The mobile industry solved this decades ago through TAP files and clearing houses; a lighter version, possibly built on the existing UPI rails, would suit PM-WANI's smaller ticket sizes.
3. **The third change relates to state government participation as PDOAs**. Paragraph 2.116 of the paper notes that Gujarat's state-supported ISP already operates as a PDOA and has demonstrated viability through aggregation. Codifying this, encouraging every state to operate or sponsor at least one PDOA at the state level, with explicit roles in PDO onboarding, technical support, and operational compliance, would convert state administrative capacity into PM-WANI capacity at marginal cost. The Gujarat experience suggests it works.

Q6. Improvements to Authentication, Authorisation, Roaming, and Payment in PM-WANI

This is the question on which Advaya has the strongest engineering view, and on which the consultation paper has done the most analytical groundwork. Paragraphs 2.130 through 2.139 of the paper effectively concede that India's continued reliance on captive portals and SMS OTP is, as the consultation paper itself acknowledges, **materially behind** global practice.

Our recommendation is unambiguous: adopt Passpoint (Hotspot 2.0) as a mandatory technical requirement for all newly deployed PM-WANI access points from a notified date, with a phased migration window of 24 to 36 months for existing hardware. Passpoint uses 802.1X/EAP-based automatic provisioning with enterprise-grade encryption. It removes the manual login step entirely, removes the OTP dependency that paragraph 2.132 itself identifies as failure-prone in cellular-congested environments, and is interoperable with cellular subscriber identity through SIM-based EAP-SIM/AKA methods. It is the standards baseline against which every serious Public Wi-Fi network in OECD economies now operates.

On payment, UPI integration at the authentication layer is the right answer for India, but with a structural qualification. The paper's framing in paragraph 2.134 leans toward a centralised authorisation, authentication, and payment gateway. We caution against full centralisation. A single national gateway becomes a single point of failure for every PM-WANI session in the country, an unacceptable resilience risk for an access layer intended to support emergency services, e-governance, and public safety use cases. A federated identity architecture, in which multiple consent-driven UPI-linked identity providers can issue and verify Passpoint credentials against a common interoperability standard, is technically equivalent in user experience and substantially more resilient.
On roaming, we treat the position under Q24 below.

Q9. Improving deployment in high-footfall outdoor and indoor scenarios
Outdoor and indoor problems are distinct, and the paper rightly separates them.

For outdoor high-footfall locations, such as bus stops, transit corridors, markets, and tourist sites, the binding constraints are power, RoW, and physical security of equipment. Each is solvable, but each requires a different agency. Aggregated bulk billing of electricity across multiple access points on the same circuit, as flagged in paragraph 2.98, is administratively a state distribution licensee matter and does not require new central legislation. **A model municipal SOP, developed jointly by the Ministry of Housing and Urban Affairs and TRAI, with deemed approvals for access points mounted on street furniture under a notified specification, would remove most of the field-level friction.**

For indoor high-footfall locations, such as airports, railway stations, metro stations, malls, hospitals, and large institutions, the paper's reference in paragraph 2.100 to its own February 2023 Recommendations on Rating of Buildings or Areas for Digital Connectivity is the most consequential cross-reference in the entire consultation. Those recommendations called for amending the Model Building Bye-Laws and the National Building Code to make Digital Connectivity Infrastructure a mandatory component of building plans on the same footing as water, electrical, gas, and fire safety. **Three years on, the central recommendation has not been adopted by the Bureau of Indian Standards into the NBC or notified in the Model Building Bye-Laws by the Ministry of Housing and Urban Affairs.**

The most useful single action TRAI could press for in its post-consultation recommendations is the operationalisation of its own February 2023 DCI recommendations, with a defined timeline. Indoor Public Wi-Fi at scale does not work without it.

A subordinate point: large indoor venues, airports, large stations, and malls should be required to support neutral-host operation. A single passive in-building infrastructure that multiple service providers and PDOAs can use eliminates significant deployment costs and prevents situations where a venue's exclusive Wi-Fi contract excludes all other providers. The paper notes this in paragraph 2.99 without making it an ask.

Q12 and Q13. Last-mile connectivity and Government funding for last-mile
We treat these together because they are the same question.

Last-mile connectivity is the binding constraint, yes. The paper's own paragraph 2.67 puts the cumulative fibre figure at approximately 42.36 lakh route kilometres at end-2025, and paragraph 2.68 reports BharatNet at 7.22 lakh kilometres connecting over 2,18,462 Gram Panchayats. The middle-mile picture is acceptable; the last-mile picture is not. Fibre that ends at the Gram Panchayat office and never extends to the village, the school, or the market is functionally absent for Public Wi-Fi.

On funding, our view is that the government should fund last-mile connectivity in genuinely uncovered or commercially unviable areas, subject to an open-access obligation. Paragraph 2.34 of the consultation paper notes that in Hong Kong, operators receiving fibre subsidies under the OFCA scheme must make at least half the subsidised network capacity available to other operators at no cost. This is a sensible model. It prevents public money from being used to build last-mile monopoly infrastructure and lowers the entry costs for PDOAs operating in areas that would otherwise depend on a single bandwidth supplier.

For the funding instrument, the Digital Bharat Nidhi is the natural vehicle; paragraph 2.111 of the paper acknowledges this. The relevant gap is operational rather than financial. DBN's current disbursement architecture is calibrated for large infrastructure tickets such as mobile tower funding and BharatNet contracts. The last-mile Public Wi-Fi extension is fundamentally different in shape: thousands of small disbursements to small operators, often at sub-₹10 lakh per site. DBN will need either a sub-window with simplified disbursement and audit rules, implementation through a state-level intermediary (states acting as PDOAs, per Q4 above), or both.

Q16. State Government initiatives for last-mile and city/town fiberisation
The paper makes an important and underappreciated observation in paragraph 2.71 that deserves to become a recommendation in its own right. Smart Cities have deployed extensive fibre and command-and-control infrastructure under the Smart Cities Mission. Paragraph 2.70 reports 7,555 projects completed, ₹1,51,361 crore deployed by May 2025, with 94% of approved projects completed. The same fibre carries CCTV, traffic systems, and command-centre data. Public Wi-Fi, which requires precisely the same fibre and power, has not been added to that infrastructure in any significant way.
This is the single largest stranded asset in the Indian Public Wi-Fi policy.

Our recommendation: **Mandate, through a directive of the Ministry of Housing and Urban Affairs in consultation with TRAI, that all existing and future Smart City fibre corridors must provision for Public Wi-Fi access points at a defined density, for example, one access point per 200 metres on major corridors and one per intersection in commercial zones, with technical specifications consistent with Wi-Fi 6E or newer**. The marginal cost of existing infrastructure is small. The political economy of the ask is easier than that of greenfield deployment because the headline projects are already complete.

Beyond Smart Cities, the SASCI guidelines of 27 March 2026, paragraph 2.113, note that ₹4,000 crore in 50-year interest-free loans to states, **linked to the implementation of the RoW Rules 2024, should be expanded to explicitly include Public Wi-Fi deployment milestones in the eligibility criteria. The lever already exists; using it to proliferate Public Wi-Fi requires only an amendment to the milestone list.**

Q22 and Q23. User authentication challenges and the case for a centralised platform
The user-experience problem and the centralisation question are connected but distinct.

From a user experience perspective, the position is clear and consistent with our Q6 response. Passpoint plus federated UPI-linked identity is the right architecture. It removes the captive portal, OTP, voucher purchase, and re-authentication on every reconnection. It does this without sacrificing security; in fact, 802.1X/EAP is materially more secure than the current OTP-and-shared-key model. Migration is the only real cost, and that cost is bounded by the device replacement cycle.

On centralisation, our position is more cautious. A fully centralised platform, a single national authentication and payment gateway operated by a single entity, concentrates risk in ways the consultation paper does not adequately discuss. *Three concerns are material.*

1. **The resilience concern is straightforward.** A single platform processing every Public Wi-Fi session in India creates a national-scale single point of failure. Even with a high availability design, the blast radius of an incident is unacceptably large for what may become public-safety-grade infrastructure.
2. **The privacy concern is structural.** Linking UPI-grade identity to every Wi-Fi session creates a continuous record of who connected where, when, for how long, and for what. Whether or not this data is technically anonymised, the architectural fact of its collection in one place creates a target for misuse.
3. **The competition concern follows from the other two.** Centralisation tends to ossify. Whichever entity operates the national platform becomes a de facto gatekeeper, and innovation in authentication and payment slows accordingly.

A federated model, multiple identity providers operating against an open Passpoint and OpenRoaming-compatible specification, with the C-DOT-operated Central Registry maintaining the trust list and certificate authority infrastructure, delivers the same user experience as full centralisation while distributing risk, preserving privacy by default, and keeping the architecture open to subsequent innovation. We recommend this in preference to a single national platform.

Q24. Interoperability, seamless roaming, and the "super-aggregator" proposal
Seamless roaming between PM-WANI hotspots should be a technical requirement of the framework, yes. We would oppose making it a regulatory mandate without first ensuring that the underlying technical and commercial mechanisms are in place.

The technical mechanism is OpenRoaming, referenced in paragraph 2.135 of the consultation paper. It is a Wireless Broadband Alliance-administered federation built on RADSEC over TLS, with a defined trust framework, certificate authority, and roaming consortium model. Multiple major operators globally are members, and the framework is interoperable with Passpoint at the device level. Mandating Passpoint plus OpenRoaming compliance for all PM-WANI deployments using public funds would deliver mandatory roaming as a consequence of standards conformance, without TRAI having to create a parallel Indian roaming framework from scratch.

We do not recommend creating a "super-aggregator" in the form proposed in paragraph 2.135 of the consultation paper. **A super-aggregator is structurally a national chokepoint.** It would replicate the centralisation risks discussed under Q23 in the roaming domain, and would substitute for a mature international framework (OpenRoaming) that India can simply join. The marginal benefit of an Indian-specific super-aggregator over OpenRoaming federation membership is unclear; the marginal cost in terms of resilience and competition is high.

The commercial mechanism is settlement, which we addressed under Q4. Without settlement economics, mandatory roaming becomes mandatory free-riding for the carrying PDOA, rapidly eroding service quality.

Q26. Additional observations
Four points that the consultation framework does not adequately surface and that we would like on record.

1. **On Wi-Fi 7 and the standards trajectory.** The paper acknowledges the evolution of Wi-Fi standards in Table B and the 6 GHz delicensing in paragraph 2.62, but does not draw a conclusion. Wi-Fi 7 (802.11be) supports multi-link operation, 320 MHz channels, and substantially higher throughput in the 6 GHz band. Deployments funded today should not be Wi-Fi 5. A standards floor for Wi-Fi 6E, with a path to Wi-Fi 7 for new public-funded deployments, is technically straightforward and economically reasonable given current hardware pricing.
2. **On V-band for outdoor mesh backhaul.** TRAI's own December 2025 recommendation to delicense the V-band (57–66 GHz), referenced at paragraph 2.62, is a major enabler for outdoor Public Wi-Fi where wired backhaul is unavailable. V-band supports multi-gigabit short-range links suitable for street-level mesh networks and the last 100 metres of backhaul. The post-consultation recommendations should reinforce expeditious operationalisation of the V-band delicensing.
3. **On convergence with 5G and 6G.** PM-WANI is treated throughout this consultation as parallel to cellular. The international direction is convergent, with 3GPP Release 16's Access Traffic Steering, Switching and Splitting (ATSSS), and the 5G non-3GPP access framework enabling Wi-Fi to function as a tightly coupled access for the 5G core. The National Broadband Mission 2.0 (paragraph 2.66) explicitly targets 6G readiness. Public Wi-Fi policy that ignores this convergence will be obsolete before it is implemented. We recommend that the post-consultation recommendations include an explicit roadmap for Wi-Fi–5G/6G convergence at the architectural level.
4. **On national branding.** Hong Kong has Wi-Fi.HK. The EU has WiFi4EU. India has PM-WANI as a backend label that no user sees, no signage carries, and no consumer recognises. A national branding programme — a single public Wi-Fi identity that users see at every hotspot, that signage carries, and that consumer education campaigns can reference is a small-cost, high-impact intervention. The absence of one is a significant contributor to the low public awareness identified in paragraph 2.93.

We support TRAI's diagnosis in this consultation and the broad direction of its policy thinking. Our specific recommendations, gathered for convenience:

Closing
1. Tie public funding to Wi-Fi 6E minimum hardware specifications, with a defined sunset for legacy equipment.
2. Mandate Passpoint (Hotspot 2.0) for all newly deployed PM-WANI access points, with a

24-to-36-month migration window for existing hardware.
3. Adopt OpenRoaming federation membership rather than creating an Indian super-aggregator. Deliver mandatory roaming through standards conformance.
4. Use a federated identity architecture for UPI-linked authentication, not a single centralised platform.
5. Operationalise TRAI's February 2023 DCI recommendations through amendments to the National Building Code and Model Building Bye-Laws, on a defined timeline.
6. Mandate the provisioning of Public Wi-Fi along Smart City fibre corridors at a defined access-point density.
7. Add Public Wi-Fi deployment milestones to the SASCI guidelines milestone list, alongside RoW Rules 2024 implementation.
8. Codify and encourage state government participation as PDOAs.
9. Publish a quarterly reference price for FTTH backhaul to PDOs, with a grievance route for non-compliance with the 2× cap.
10. Develop a positive list of permitted indirect monetisation models for PDOAs, with corresponding consent and data-handling obligations.
11. Operationalise expeditiously the December 2025 V-band delicensing recommendation for outdoor mesh backhaul.
12. Include Wi-Fi-5G/6G convergence in the post-consultation architectural recommendations.
13. Establish a national Public Wi-Fi branding programme.

Warm regards,
Aditya

Aditya Chaudhuri
Founder & CTO, Advaya Networks Pvt. Ltd.
Senior Member, IEEE · Fellow, IETE · Fellow, IE(I)
Adjunct Professor of Practice, IIT Mandi (SCEE)
Email: aditya.chaudhuri@advayanet.ai · Mobile: +[redacted]