CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT

Comments on

Consultation Paper On the "Proliferation of Public Wi-Fi Networks in India"

Introduction :

The underscores that broadband today is not merely a telecommunications service but a foundational digital infrastructure comparable to electricity and transport in its enabling role across the economy. It drives inclusive growth, strengthens governance, supports Digital Public Infrastructure, and enables emerging technologies such as Artificial Intelligence, cloud computing, and digital commerce. In this evolving landscape, Public Wi-Fi represents a critical last-mile and access-layer solution that can bridge the gap between high-capacity fixed broadband and the need for affordable, ubiquitous wireless connectivity.

India has made remarkable progress in expanding digital connectivity through widespread 4G deployment, rapid growth in smartphone adoption, and globally competitive data tariffs. However, the consultation paper rightly highlights that significant disparities persist in terms of access, quality of service, and meaningful usage across rural, semi-urban, and

dense urban environments. While mobile broadband provides wide-area coverage, it faces inherent capacity constraints, congestion challenges, and variability in performance, particularly in high-density and high-demand environments. Public Wi-Fi, operating on unlicensed spectrum and anchored on fixed broadband backhaul, offers a complementary and cost-efficient mechanism to address these limitations and to enable scalable, high-capacity connectivity in shared public spaces.

The introduction of the PM-WANI framework marked a progressive step towards democratizing internet access by enabling small entrepreneurs, local entities, and community-based operators to participate in the broadband ecosystem without onerous licensing barriers. This unbundled architecture has the potential to create a distributed, inclusive, and innovation-driven connectivity model. However, as also recognized in the consultation paper, the proliferation of Public Wi-Fi networks has not yet reached the scale envisaged, due to structural challenges including weak commercial viability, fragmented implementation, backhaul constraints, limited participation of State and local bodies, and concerns relating to security, privacy, and user trust.

From a policy perspective, the next phase of Public Wi-Fi expansion in India must therefore move beyond a narrow infrastructure-centric approach and adopt a **holistic, ecosystem-based strategy** that aligns the incentives of all stakeholders. This includes consumers, Public Data Offices (PDOs), PDO Aggregators (PDOAs), Internet Service Providers (ISPs), Telecom Service Providers (TSPs), infrastructure providers, device manufacturers, content platforms, State Governments, Urban Local Bodies (ULBs), and private

investors. The success of Public Wi-Fi depends not only on deployment but also on sustained usage, service quality, affordability, and trust.

International experience provides valuable insights in this regard. Advanced digital economies have adopted differentiated, context-specific models to scale Public Wi-Fi. The European Union has focused on publicly funded community Wi-Fi with strong emphasis on backhaul and municipal participation. South Korea has integrated Public Wi-Fi as part of its national digital infrastructure strategy with dense urban coverage and high quality of service. Singapore has implemented a neutral-host, interoperable Wi-Fi ecosystem with seamless authentication and strong security standards. Similarly, countries like Brazil and Indonesia have leveraged targeted subsidies and public funding to extend connectivity to remote and underserved regions. These models demonstrate that successful proliferation requires a combination of public investment, private participation, regulatory facilitation, and consumer-centric design.

In the Indian context, Public Wi-Fi must be viewed as a **strategic enabler of digital inclusion, economic productivity, and network efficiency**. It has the potential to:

- Enhance affordability of internet access, particularly for low-income users, students, gig workers, and MSMEs
- Offload traffic from mobile networks, thereby improving overall quality of service and spectrum efficiency
- Enable high-capacity connectivity in high-footfall areas such as railway stations, markets, campuses, and hospitals

- Support delivery of e-governance services, digital payments, telemedicine, and online education
- Bridge the rural-urban digital divide through community-based access models

At the same time, the proliferation of Public Wi-Fi must be anchored in **consumer protection, transparency, and trust**. Users must be assured of data privacy, secure authentication, non-discriminatory access, and predictable quality of service. Without these safeguards, adoption will remain limited regardless of infrastructure expansion.

A forward-looking regulatory approach must therefore be guided by the following core principles:

- **Equity and Inclusion:** Ensuring access for underserved and vulnerable populations
- **Economic Sustainability:** Enabling viable business models for PDOs and ecosystem participants
- **Technology Neutrality:** Supporting multiple access and backhaul technologies, including fibre, satellite, and wireless
- **Interoperability and Open Access:** Promoting seamless user experience across networks
- **Consumer Protection and Trust:** Embedding privacy, security, and transparency into the ecosystem
- **Collaborative Governance:** Aligning roles across Centre, States, and local bodies

The consultation paper rightly calls for a reassessment of regulatory, economic, and operational frameworks governing Public Wi-Fi. In this

context, it is imperative to adopt a **differentiated, stakeholder-aligned, and future-ready policy architecture** that reflects India's diverse geography, demand patterns, and socio-economic realities.

Public Wi-Fi, if designed and implemented effectively, can evolve into a foundational pillar of India's digital ecosystem—complementing mobile broadband, enhancing fixed broadband utilisation, and enabling universal, affordable, and high-quality internet access. The present consultation therefore offers a critical opportunity to shape a scalable, resilient, and inclusive Public Wi-Fi ecosystem that aligns with India's long-term vision of Digital India and global digital leadership.

Issues for Consultation :

Q1. What are the key supply-side constraints affecting Public Wi-Fi proliferation in India? What targeted policy or regulatory measures may be required to address these supply-side constraints? Please provide your response in detail with justification.

Comments :

What are the key supply-side constraints affecting Public Wi-Fi proliferation in India?

Comments :

Comment on Supply-Side Constraints Affecting Public Wi-Fi Proliferation in India :

This submission respectfully submits that the central supply-side problem is no longer the absence of a policy framework for Public Wi-Fi, but the gap between a liberalized framework and the on-ground economics, infrastructure,

standards, and institutions required to scale it. India's National Digital Communications Policy 2018 set a target of 10 million public Wi-Fi hotspots by 2022, yet the Department of Telecommunications-enabled PM-WANI ecosystem had reached about 410,131 hotspots by April 2026, while TRAI's performance indicators showed 55,483 TSP/ISP public Wi-Fi hotspots as of December 2025. These counts are not directly additive because they use different reporting definitions, but together they show that India remains far below its original public Wi-Fi ambition.

Defining the Problem Clearly

The core issue is that India has liberalized entry for hotspot provision, but has not yet made supply scalable, predictable, and commercially durable at the last mile. TRAI's consultation paper states that hotspot density and operationalization remain below global peers; it also identifies persistent last-mile fiber gaps, non-uniform implementation of the 2024 Right of Way rules, high and variable charges, overlapping clearances, and timeline uncertainty as major impediments to Wi-Fi deployment. In other words, Public Wi-Fi has been deregulated at the edge, but it is still constrained in the backhaul, permissions, and operations layers.

This matters for consumers because Public Wi-Fi is a complementary access layer for shared spaces, indoor coverage, dense-user environments, and low-income or device-constrained users. It matters for industry because it can offload traffic, extend broadband deeper into neighborhoods and villages, and enable digital commerce in markets, transport hubs, schools, clinics, and community institutions. It matters for national goals because Digital India seeks a digitally empowered society and knowledge economy, while NBM 2.0 is explicitly aimed at high-speed broadband and meaningful connectivity for all,

with special emphasis on rural and remote areas and on a digital map of PM-WANI and other telecom assets.

The supply constraint is also economic. India had 1,028.61 million internet subscribers by December 2025, but only 45.32 million were fixed broadband subscribers, or about 4.4% of the total. At the same time, average wireless data usage reached 25.70 GB per data subscriber per month, while average wireless data realization was only Rs 7.87 per GB. This combination means that the fixed backhaul base available to small venues is still thin, while mobile data is so cheap and seamless that many Public Wi-Fi sites struggle to monetize. That weakens the business case for small Public Data Offices even where the legal entry barrier is low.

The constraints can be grouped as follows:

- **Technical constraints.** PM-WANI lowered entry barriers, but India still relies heavily on OTP and captive-portal style onboarding. TRAI notes that this legacy approach creates friction, while seamless roaming remains limited and India has not yet embedded Passpoint/OpenRoaming-like interoperability in mainstream deployments.
- **Regulatory and institutional constraints.** RoW implementation remains uneven across states and municipalities; permissions often involve multiple agencies; and local bodies control key assets such as poles, bus shelters, public buildings, and street furniture. TRAI also recognizes that system integrators can reduce deployment complexity, but that function is not yet structurally embedded in the ecosystem.
- **Economic constraints.** The DoT's 2024 PM-WANI reforms and TRAI's 2025 tariff cap were needed precisely because high internet costs and expensive connection arrangements were discouraging small businesses

from becoming PDOs. Even after those reforms, low hotspot revenues, consumer expectations of free access, and competition from cheap mobile data continue to compress margins.

- **Operational and geographic constraints.** As of November 2025, more than 50.6% of PM-WANI hotspots were in Delhi alone, and the top five states accounted for roughly 81.4% of all PM-WANI hotspots, showing deep geographic concentration. Separately, BharatNet had over 1,04,574 installed Wi-Fi hotspots as of May 2025, but PRS Legislative Research reported that Wi-Fi was active in only 766 gram panchayats as of September 2025, indicating a severe operations and utilization gap.

Exploring All Possible Solutions

Infrastructure and backhaul reform

The first pathway is to treat Public Wi-Fi as a last-mile broadband use case that depends on frictionless access to backhaul and public assets. This requires strict implementation of the Telecom Right of Way framework, a single digital workflow for approvals, standard municipal permissions for poles and street furniture, and broader use of multi-technology backhaul including fiber, microwave, mobile backhaul, and satellite where fiber is not immediately economic. This pathway addresses the most load-bearing supply constraint because no hotspot architecture scales if every venue must negotiate costly, slow, and uncertain infrastructure access.

Sustainable economics for PDOs and neutral-host models

The second pathway is to strengthen venue-level economics. The DoT's 2024 reforms already allow a regular FTTH connection for PDOs, aggregated backhaul for multiple access points, dual-SSID participation from home or business Wi-Fi,

roaming across PDOAs, and mobile-data offload tie-ups. TRAI's 2025 tariff order then capped PDO FTTH pricing up to 200 Mbps at no more than twice the corresponding retail tariff. These are sound steps and should now be institutionalized through standard PDO products, standard wholesale SLAs, and targeted rather than blanket subsidy for low-income and rural clusters. In uncovered areas, Digital Bharat Nidhi support should be linked to performance and to specific anchor sites such as schools, PHCs, transport hubs, and panchayat campuses.

Standards-based interoperability and lower-friction onboarding

The third pathway is a technical modernization from "best effort hotspot" to "carrier-grade public Wi-Fi." The Central Registry run by entity ["organization","C-DOT","india telecom r&d"] already provides a discovery and interoperability foundation, but TRAI has correctly observed that OTP-based onboarding and non-standard roaming create structural friction. India should therefore move toward a standards profile that supports WPA3, 802.1X/EAP, Passpoint-compatible onboarding, interoperable roaming, and UPI-linked consent-based authorization and payment. This directly addresses both supply and demand: operators gain better conversion, session continuity, and lower support costs, while consumers get a more cellular-like experience.

Institutional delivery through system integrators and anchor deployments

The fourth pathway is to recognize that many venue owners, panchayats, schools, hospitals, small shops, and market associations cannot design, deploy, secure, and maintain Wi-Fi systems themselves. TRAI explicitly notes that system integrators can combine access points, switches, backhaul, authentication, cybersecurity, and analytics into one deployable solution, reducing complexity and providing a single point of accountability. India should

therefore create a formal system-integrator layer for public Wi-Fi procurement and maintenance, especially for state and municipal projects and for BharatNet-linked village clusters.

Venue incentives, property readiness, and public-asset participation

The fifth pathway is to create a venue-side incentive framework. TRAI's digital connectivity rating framework already recognizes fiber readiness, in-building coverage, Wi-Fi infrastructure, speeds, and user experience, and its 2025 manual underscores that in-building connectivity is now essential because more than 80% of mobile data is consumed indoors. This framework can be extended from a consumer information tool into a supply-side accelerator by encouraging or requiring Wi-Fi-ready public buildings, hospitals, transport hubs, campuses, and large commercial venues. Internationally, the European Commission[16]'s WiFi4EU model funded equipment and installation through vouchers while municipalities paid connectivity and maintenance for three years, and the municipal model in Seoul has been built on city-owned broadband infrastructure and now covers over 35,000 public Wi-Fi units. These examples show that public policy works best when it socializes site readiness and basic capex, while keeping operations disciplined and accountable.

Global best-practice lessons relevant to India

The most relevant global lessons are not "free Wi-Fi everywhere" slogans, but specific design choices. Singapore's Wireless@SG uses a federated model sustained commercially between venue owners and operators, while the IMDA enforces consistent standards for login, identity management, security, and roaming. The UK's GovWifi model shows that single sign-up and automatic reconnection can be layered over existing infrastructure, reducing administrative burden. And the Wireless Broadband Alliance's OpenRoaming

framework shows how large-scale secure roaming can be achieved through cloud federation, cybersecurity, and network automation. India should adapt these principles, not copy them mechanically: federated governance, standards-based onboarding, and shared infrastructure are the transferable lessons.

Evaluating the Options

Option A: RoW, backhaul, and public-asset access reform. Feasibility is high because the legal and policy base already exists in the Telecom Act, the RoW Rules, and NBM 2.0; what is missing is consistent state and local implementation. Cost implications are moderate and largely administrative, with some fiscal implications if states rationalize charges or open municipal assets on facilitative terms. Consumer impact is high because this option improves coverage, uptime, and speed at the foundation layer. Regulatory alignment is very strong. The main risk is state or municipal resistance, especially where permissions are still treated as a revenue source rather than an enabling function. Long-term sustainability is high because cheaper and faster site rollout permanently improves network economics.

Option B: Strengthened PDO economics through tariff discipline, shared backhaul, and targeted viability support. Feasibility is also high because DoT and TRAI have already taken initial steps. Cost implications are low-to-moderate if the strategy relies mainly on wholesale product design and targeted Digital Bharat Nidhi support instead of across-the-board subsidy. Consumer impact is high in underserved areas and moderate in dense urban zones, where economics are already better. Regulatory alignment is strong with NDCP 2018, PM-WANI, and the consumer interest logic behind TRAI's tariff cap. Risks include subsidy leakage, support to non-performing sites, and overdependence on promotional revenue streams. Sustainability is good only if support is targeted

and time-bound, and only if it is paired with interoperability and easier onboarding.

Option C: Standards-based upgrade to secure, seamless, interoperable Wi-Fi. Feasibility is moderate: technically it is straightforward because global standards already exist, but migration requires certification, device compatibility management, and ecosystem coordination. Cost implications are moderate in the short run because networks, controllers, apps, and support systems will need upgrades, but those costs should fall over time as interoperability reduces friction and support overhead. Consumer impact is extremely high because the main experiential weakness of public Wi-Fi in India is not only price but hassle. Regulatory alignment is strong with PM-WANI's interoperability logic, with data-protection and cybersecurity requirements, and with international standards. Risks include legacy-device compatibility and slower uptake by very small operators unless turnkey solutions are available. Long-term sustainability is extremely high because this option turns Wi-Fi from a stop-gap utility into a trusted access layer.

Option D: Venue incentives, digital-connectivity ratings, and anchor-site obligations.

Feasibility is moderate because this requires coordination with states, local bodies, transport agencies, health and education departments, and large private venues. Cost implications are variable: light-touch rating and approvals are inexpensive, while anchor-site deployment requires real capex and opex. Consumer impact is high because it improves connectivity where people actually live, travel, study, and access services. Regulatory alignment is strong with Digital India, NBM 2.0, and TRAI's digital-connectivity framework. Risks include uneven implementation and the creation of isolated "showcase" sites unless

interoperability is built in from the start. Sustainability is good where anchor institutions guarantee traffic and where procurement includes maintenance and uptime commitments.

Option E: Formal use of system integrators and managed service models. Feasibility is high because the capability already exists in the market; the missing element is institutional recognition and common procurement standards. Cost implications are moderate but efficient, because integration costs usually replace fragmented and repeated troubleshooting costs. Consumer impact is indirect but important, as better deployment and maintenance translate into fewer dead hotspots and more consistent quality. Regulatory alignment is high, especially for public projects and BharatNet-linked last-mile models. Risks include vendor lock-in if standards are not open and procurements are not neutral. Long-term sustainability is high if interoperable architectures and performance-linked contracts are used.

Making a Judgment

The best course is not a single option, but a sequenced combination led by **Option A and Option C**, supported by **Option B**, and operationalized through **Option D and Option E**. The reason is straightforward: India's biggest bottlenecks are still last-mile economics and implementation friction, but making backhaul cheaper will not by itself create a scaled public Wi-Fi ecosystem if users still face OTP delays, repeated logins, fragmented roaming, weak trust, and inconsistent quality. Conversely, a sophisticated standards framework will not scale if venues cannot get affordable backhaul and permissions. The correct regulatory judgment is therefore to tackle infrastructure friction and technical friction together, while limiting public subsidy to locations where the market alone will not deliver.

This combined approach is consumer-first because it aims to improve affordability, usability, trust, and grievance redressal simultaneously. It aligns with NDCP 2018 because it revives the public-Wi-Fi objective through lighter compliance and wider participation. It aligns with Digital India because it extends digital infrastructure into everyday public and community spaces. It aligns with NBM 2.0 because the Mission expressly targets universal, affordable, and meaningful connectivity, better RoW implementation, and a national digital map of telecom assets including PM-WANI. It also aligns with modern international standards because WPA3, enterprise authentication, Passpoint-type onboarding, and OpenRoaming-style federation are all consistent with secure and scalable public access.

It is equally important that India resists two policy mistakes. The first would be to assume that deregulation alone is enough; the evidence of hotspot concentration, last-mile gaps, and uneven operations shows that it is not. The second would be to rely on blanket subsidies or fully free models everywhere; a more durable strategy is to use targeted support in underserved locations, while re-engineering the economics and user experience in commercially viable areas. The goal should be a mixed ecosystem: free where the public-interest case is strongest, freemium where anchor institutions can subsidize access, and paid where venues can sustain differentiated service.

Forward-Looking Implementation Plan

Short-term actions

Within the next 12 months, TRAI should recommend a national Public Wi-Fi implementation package centered on enforceable RoW outcomes, not just high-level principles. This package should include: a public state/UT scorecard on RoW timelines and charges affecting Wi-Fi backhaul; a model framework for

municipal access to poles, shelters, public buildings, and street furniture; mandatory publication of PDO backhaul offers and SLA terms by access providers; and standardized consumer disclosures on price, speed, validity, fair-use limits, complaint contacts, and data practices. At the same time, DoT should update PM-WANI technical specifications so that new public-interest deployments are Passpoint-ready, roaming-capable, UPI-integrated, and security-baselined from day one.

In the same period, DoT and C-DOT should enhance the Central Registry into a true transparency layer by publishing a verified national hotspot map showing location, operational status, PDOA, and—at least for publicly supported hotspots—basic uptime and complaint metrics. ISPs and TSPs should be required, or strongly nudged, to offer simple PDO broadband products consistent with the tariff cap and with standardized onboarding. State governments and local bodies should identify priority anchor locations such as bus stands, railway stations, hospitals, schools, colleges, courts, markets, tourism sites, and panchayat campuses for the first wave of interoperable deployments.

Medium-term actions

Over one to three years, India should shift from hotspot registration growth to hotspot performance growth. That means linking public support to measured outcomes such as uptime, average sessions, complaint closure, and backhaul availability. Digital Bharat Nidhi support should be used to create district-level or cluster-level viability-gap programs in uncovered and underserved areas, especially where BharatNet backhaul exists but operations are weak. The BharatNet Udyami model offers a useful template because it ties local

entrepreneurship to last-mile delivery and ongoing upkeep rather than just one-time installation.

India should also institutionalize a system-integrator layer. TRAI and DoT can encourage standard procurement templates, open-interface requirements, and empanelment norms so that state agencies, smart-city SPVs, schools, hospitals, and municipalities can buy a managed Wi-Fi outcome rather than assemble a patchwork of hardware and software. In parallel, the digital-connectivity rating framework should be extended through state byelaws, concessions, or procurement conditions so that large buildings and transport/public-service properties become “Wi-Fi ready by design.”

Long-term actions

Over three to five years, India should aim for a federated, neutral-host public Wi-Fi fabric that feels seamless to the user and modular to the provider. In such a model, a user can discover and join approved networks securely with minimal friction, while providers can choose among multiple backhaul technologies, service integrators, and revenue models. Public Wi-Fi should become a normal extension of India’s broader broadband strategy, not a niche program. As the policy framework around additional unlicensed capacity matures, India should remain technology-neutral and permit newer Wi-Fi generations to improve performance in dense indoor and community settings.

Roles of stakeholders

TRAI should lead on tariff oversight, transparency, interoperability recommendations, consumer disclosure norms, and state-level implementation scorecards. DoT should lead on PM-WANI standards, Central Registry modernization, RoW portal alignment, inter-ministerial coordination, and

targeted Digital Bharat Nidhi support. ISPs and TSPs should provide compliant PDO connectivity products, honor shared-backhaul and dual-SSID models, and build offload and roaming partnerships where commercially sensible. States and local bodies should align RoW practices, open public assets, rationalize local charges, and integrate public Wi-Fi into urban planning and public-service delivery. Industry associations and standards bodies should support turnkey templates, certification, small-operator training, and open technical profiles that avoid lock-in.

Monitoring, transparency, and consumer-protection mechanisms

Consumer protection must be built into the supply architecture. Every PDOA-facing service should provide clear pre-access disclosure of price, validity, expected speeds, data caps, complaint channels, and what personal data is collected. Promotional messaging should be opt-in and separate from basic access consent. Complaints should be mandatorily handled through the PDOA layer with time-bound resolution standards. Publicly funded or publicly hosted hotspots should publish uptime and complaint statistics. Security and privacy should follow a privacy-by-design approach consistent with the Digital Personal Data Protection Act, 2023, PM-WANI's local-data and logging obligations, and CERT-In's cybersecurity directions.

Open Questions and Data Limitations

Current reporting still has material gaps. India uses different reporting units across PM-WANI hotspots, TSP/ISP hotspots, access points, railway-station Wi-Fi sites, and BharatNet gram-panchayat Wi-Fi, so aggregate "national hotspot totals" should be used carefully. More importantly, registration counts do not reveal uptime, quality, traffic, or sustained usage. Future regulatory monitoring should therefore distinguish between **installed**, **registered**,

operational, and **actively used** hotspots, because supply-side policy should be judged by reliable service delivered to consumers, not by headline installation counts alone.

What targeted policy or regulatory measures may be required to address these supply-side constraints? Please provide your response in detail with justification.

Comments :

Comment on Targeted Policy and Regulatory Measures to Address Supply-Side Constraints in Public Wi-Fi Proliferation in India

Problem Definition

India's core policy problem is no longer the absence of a Public Wi-Fi framework; it is the gap between a permissive framework and scaled, sustainable deployment. The National Digital Communications Policy 2018 set a target of 10 million public Wi-Fi hotspots by 2022, with NagarNet and JanWiFi intended to expand urban and rural access. Yet, as of 28 February 2026, PM-WANI had 4,09,403 operational Public Data Offices and hotspots, 207 PDOAs, and 113 App Providers—roughly 4 percent of the NDCP target—despite having reached 2,44,67,896 users and 58.64 petabytes of cumulative data consumption. That gap shows that the problem is not conceptual demand for affordable broadband; it is supply-side friction in deployment economics, backhaul, interoperability, and local execution.

The supply-side constraints can be grouped into five categories.

Technical constraints

Include inadequate last-mile fiber, expensive backhaul, limited access to street furniture and power, inconsistent indoor design readiness, and the absence of default interoperability, persistent authentication, and seamless roaming across hotspots.

Economic constraints

Include thin hotspot-level margins because recurring costs for backhaul, electricity, maintenance, and revenue-sharing often exceed predictable revenues, especially where users already have low-cost mobile data.

Regulatory and institutional constraints

Fragmented municipal permissions, uneven implementation of right-of-way norms, lack of standardized wholesale PM-WANI offers, and the still-incomplete use of license-exempt and shared-spectrum tools to reduce deployment cost.

Operational constraints

Include inconsistent hotspot quality, weak maintenance incentives, and non-standardized onboarding and grievance flows.

Ecosystem constraints

Include low awareness among small businesses and community institutions that they can operate as PDOs, limited financing for MSME-scale deployments, and insufficient demand aggregation by public institutions and urban local bodies. TRAI's consultation paper explicitly identifies the last-mile, security, privacy, authentication, roaming, awareness, and outdoor deployment problems as major barriers to scale.

This matters directly for consumers and national digital goals. For consumers, slow hotspot rollout means fewer affordable access points in markets, transport hubs, schools, hospitals, and community spaces, especially where households still depend on shared or outside-the-home connectivity. For industry, it means a large stranded opportunity in Wi-Fi offload, local entrepreneurship, neutral-host models, and venue connectivity. For the state, it means slower progress toward Digital India, NDCP 2018's broadband goals, and the National Broadband Mission 2.0 objective of "high-speed broadband and meaningful connectivity for all," particularly in rural and remote areas where public or shared access can complement household and mobile broadband rather than substitute for it.

Targeted Policy and Regulatory Measures :

Preserve the light-touch PM-WANI entry framework, but simplify operating compliance further. The starting principle should be regulatory non-regression:

1. **India should not reintroduce licensing burdens for PDOs** when the current framework already allows any entity to become a PDO without DoT registration, and allows PDOAs and App Providers to register without fees under a deemed-registration model. The targeted reform now needed is not a new licence class, but a standardized operating toolkit: model contracts between PDOs and upstream providers, common API and certification profiles, downloadable implementation templates, and a single digital compliance dashboard for PDOAs. That would reduce transaction costs without raising entry barriers for kirana stores, community institutions, or MSMEs.

2. **Move from passive tariff relief to an open-access backhaul regime for Public Wi-Fi.** TRAI's 2025 tariff order was an important corrective: it responded to the problem of expensive Internet Leased Lines and now requires FTTH plans up to 200 Mbps for PDOs at tariffs not exceeding twice the corresponding retail FTTH tariff. But that should be treated as a floor, not the end-state. TRAI should recommend a published reference-offer framework under which TSPs and ISPs disclose PM-WANI backhaul products, installation charges, uptime commitments, contention assumptions, repair timelines, and migration paths from entry plans to higher-capacity plans. In parallel, DoT should require BharatNet and state fiber networks to provide non-discriminatory, open-access PM-WANI backhaul products at digital public infrastructure sites, especially schools, health centres, panchayat buildings, bus stands, railway-adjacent areas, and municipal markets.
3. **Use targeted public support only where private deployment is not commercially viable.** A consumer-first and fiscally prudent approach is to reserve Digital Bharat Nidhi support, state grants, or Smart Cities funds for places with clear social value but weak standalone revenue: rural public institutions, tribal blocks, border villages, large bus depots, district hospitals, public libraries, and dense low-income settlements. Support should be outcome-based rather than equipment-based: subsidy per verified active hotspot, per uptime threshold met, or per eligible user session delivered, instead of blanket CAPEX reimbursement. This lowers the risk of idle infrastructure and aligns payment with consumer benefit.

4. **Adopt a spectrum roadmap that is explicitly pro-Wi-Fi and technologically neutral.** India has already delicensed the lower 6 GHz band from 5925–6425 MHz for low-power indoor and very-low-power outdoor use on a shared, non-interference basis. TRAI has also noted its recommendation to delicense V-band spectrum for low-power indoor and very-low-power outdoor use, which is highly relevant for dense Wi-Fi mesh and short-range multi-gigabit links. The next step should be a staged roadmap: protect and operationalize lower 6 GHz immediately; expand low-friction access to E-band and V-band for backhaul; and launch controlled pilots for database-assisted sharing and AFC-style coexistence models in additional bands where incumbent protection is required. This would create a policy pipeline for future Wi-Fi 6E/7 scale-up without committing India to a single spectrum architecture prematurely.
5. **Turn optional roaming into default interoperability.** PM-WANI currently permits bilateral roaming arrangements between PDOAs, but a permissive rule is not the same as a usable national roaming fabric. TRAI should recommend default interoperability obligations for all certified PDOAs through common authentication, settlement, and roaming interfaces. The architecture should move away from repeated captive-portal logins and toward device-based or profile-based onboarding using Passpoint/Hotspot 2.0-compatible methods, with identity federation modeled on OpenRoaming-type principles where feasible. The regulatory objective should be simple: one-time onboarding, encrypted access, persistent credentials, and seamless switching across hotspots from different providers.

6. **Upgrade security and authentication from a compliance obligation to a trust-building framework.** TRAI's consultation paper is correct that trust deficits are now a deployment constraint as much as a user problem. A national baseline should therefore require encrypted hotspot access wherever device support permits, stronger EAP-based authentication options, client isolation, signed network profiles, transparent privacy notices, and minimum cyber-incident response obligations at PDOA level. That framework should align with India's existing legal architecture on telecom operations, data protection, and cyber incident handling, including PM-WANI's current requirements on complaint handling and data/log storage within India. Security obligations should be graduated by scale so that they remain proportionate for small operators, but the consumer should receive the same minimum protections regardless of who owns the hotspot.
7. **Use municipal reform as a deployment accelerator, not an afterthought.** Outdoor Wi-Fi proliferation depends heavily on access to poles, bus shelters, public buildings, utility corridors, and low-friction permissions. The Telecommunications Right of Way Rules 2024 already provide a stronger foundation, including digital processing, deemed permission timelines, and limits on what public entities may charge. TRAI should recommend a Public Wi-Fi deployment protocol under those rules: bulk applications for hotspot corridors, standard street-furniture tariffs for Wi-Fi use, single-window electricity arrangements, common trenching or shared ducts wherever feasible, and mandatory publication by ULBs of hotspot-ready public assets. In short, India should treat Public Wi-Fi as a

public-utility layer that may ride on municipal assets under clear, non-discriminatory terms.

8. **Strengthen local entrepreneurship and MSME economics around PDOs and PDOAs.** The framework already intends to enable small and local actors, but the remaining problem is activation. DoT and industry bodies should co-develop a PDO starter pack: template business models, standard tariffs, simple accounting tools, low-cost Wi-Fi equipment catalogues, multilingual onboarding, credit products for small deployments, and training delivered through CSCs, industry associations, and state IT missions. The April 2026 government statement is useful here because it already signals policy support for mobile data offloading, branded content with user consent, FTTH-based service, and multiple access points per backhaul link. The regulatory task is therefore to make those flexibilities usable for small providers, not just legally available on paper.
9. **Promote shared infrastructure and neutral-host models in high-footfall indoor venues.** Railway stations, metro stations, airports, malls, colleges, hospitals, courts, district offices, and convention centres often have the traffic density to support Wi-Fi, but only if duplication is minimized. TRAI should support neutral-host in-building Wi-Fi systems that multiple service providers can use through shared access, especially where venue owners are public authorities. This is more efficient than each operator building parallel networks, and it aligns with both NDCP 2018's infrastructure-sharing logic and the consultation paper's own recognition that indoor, high-density environments need denser AP layouts and more careful design.

Evaluate Each Policy Option

1. **Regulatory simplification and standardized onboarding.** Feasibility is high because the legal architecture is already light-touch and in force; the reform is mostly administrative and technical. Cost implications are low for government and modest for PDOAs that must align systems and templates. Consumer benefit is indirect but meaningful because lower entry friction usually increases hotspot density faster than formal subsidy alone. Regulatory alignment is strong because the measure deepens—not reverses—the current PM-WANI philosophy. The main risk is that simplification without quality controls could permit inconsistent service experience, but that can be managed through certification and dashboard-based oversight. Long-term sustainability is high because it lowers recurring transaction costs rather than depending on permanent fiscal support.

2. **Open-access backhaul and targeted public support.** Feasibility in India is medium to high: the tariff framework already exists, BharatNet and state fiber assets are already deployed, and NBM 2.0 explicitly prioritizes broadband expansion and infrastructure coordination. Cost implications are mixed: reference offers and transparency obligations are low-cost, but viability-gap funding and open-access provisioning in remote areas require real public spending and operational oversight. Consumer benefit is very high because lower backhaul cost translates directly into more hotspots, better speeds, and wider rural and institutional reach. The principal risk is subsidy leakage or underused assets if support is not tied to real service delivery. Long-

term sustainability is therefore strong only if support is targeted, time-bound, and linked to measurable uptime and usage.

3. **Spectrum expansion, shared-spectrum tools, and wireless backhaul reform.** Feasibility is medium because spectrum decisions require careful coexistence analysis and may involve incumbent users. Fiscal cost is low compared with trenching and fiber CAPEX, which makes this option attractive as a cost-reduction lever. Consumer benefit is moderate to high: it improves hotspot performance, enables lower-cost deployment, and provides faster scale-up in places where fiber or leased access is expensive. Risks include interference, equipment fragmentation, or over-optimistic assumptions about database coordination. Regulatory alignment is strong because NDCP 2018 already calls for light-touch licensing, more spectrum for broadband, and dynamic database systems, and India has already taken a concrete step by delicensing lower 6 GHz. Sustainability is high if expansion is sequenced, standards-based, and tied to coexistence evidence.
4. **Interoperability, roaming, and simplified authentication.** Feasibility is high on the software and standards side, though not trivial operationally because PDOAs will need common settlement, identity, and profile management. Costs are moderate and mainly borne once—in backend upgrades, credential systems, and certification—rather than continuously. Consumer impact is exceptionally high because repeated logins, discovery friction, and inconsistent onboarding are among the biggest barriers to actual use. Risks include cyber-security exposure if federation and credentialing are poorly implemented, but those risks are lower under encrypted,

standards-based approaches than under open captive-portal models. Long-term sustainability is very high because this option simultaneously raises usage, improves venue value, and makes PM-WANI more competitive with mobile broadband on convenience rather than just price.

5. **Security and consumer-protection baseline.** Feasibility is medium: the obligations are implementable, but they must be proportionate to avoid overwhelming small PDOs. Cost implications are low to moderate, depending on whether encryption, RADIUS/EAP, logging, and incident-response tooling are deployed through PDOAs as shared services rather than individually by each PDO. Consumer benefit is high because trust is a precondition for sustained use, especially for education, payments, e-governance, health access, and other sensitive transactions. Risks include compliance creep and unnecessary complexity if mandates are too prescriptive. Alignment with NDCP 2018's "Secure India" mission is strong, as is alignment with existing cyber-incident and privacy obligations. Sustainability is high if enforcement focuses on PDOA-level shared controls, standardized notices, and auditable minimums rather than bespoke paperwork for every small hotspot owner.
6. **Municipal access reform, PPPs, and entrepreneurship enablement.** Feasibility is medium because it depends on Centre-State-local coordination, but the RoW framework and NBM 2.0 have already created a policy basis for it. Costs vary: publishing asset inventories and bulk permitting are low-cost; PPP vouchers and corridor models require some public or venue-owner support. Consumer benefit is high in practice because many of the most

valuable hotspots are in municipally controlled or institutionally managed spaces. Risks include slow state-level uptake, uneven implementation quality across cities, and the possibility that some “free Wi-Fi” projects become financially weak after the first rollout cycle. Sustainability is therefore best when PPPs use shared infrastructure, open-access models, and clear O&M responsibility rather than one-time procurement-led deployment.

Integrate International Best Practices :

The most useful lesson from the entity ["organization","Federal Communications Commission","us communications regulator"] is not that India should copy the United States wholesale, but that shared-spectrum and database-assisted approaches can create more capacity without turning every band into a high-cost auction product. In CBRS, General Authorized Access users can operate across 3550–3700 MHz subject to protecting incumbents and priority users, while the FCC has also approved multiple Automated Frequency Coordination systems for commercial 6 GHz operation. India can adapt that lesson by piloting AFC-style coexistence only where it materially lowers deployment cost and where incumbent protection is technically credible.

The most practical lesson from the entity ["organization","European Commission","eu executive body"] is the municipal voucher model. WiFi4EU gave municipalities vouchers worth €15,000 to install Wi-Fi in public spaces, and the programme has since supported more than 7,200 municipalities and over 93,000 hotspots. India should not replicate that instrument indiscriminately, but it should adapt the logic: small, standardized, time-bound public support for venue installation in places with clear public value

and weak private returns. That is especially relevant for district-level public institutions and smaller urban local bodies.

The lesson from entity ["organization","Infocomm Media Development Authority","singapore regulator"] is that public Wi-Fi becomes durable when it combines a federated commercial model with common standards for identity, login, security, and user experience. Wireless@SG sustains hotspots commercially between venue owners and operators, while still enabling seamless roaming and standardized identity management; it also supports easier login with EAP-SIM, app-based auto-connect, SMS OTP for local and foreign users, and minimum service benchmarks. India should adapt that approach by making PM-WANI a truly federated, interoperable public access layer rather than a set of technically compliant but user-fragmented islands.

The combined lesson from entity ["city","Tokyo","japan"] and entity ["city","Seoul","south korea"] is that mature public Wi-Fi policy shifts from “install more endpoints” to “ensure secure auto-connect and reliable quality.” Tokyo’s current public Wi-Fi experience uses one-time setup, encrypted access, and OpenRoaming-compatible logic for automatic reconnection, while Seoul is explicitly upgrading public Wi-Fi quality through Wi-Fi 7, integrated management, and investment in high-value tourist and public-service areas. The broader structural enabler in South Korea is also important: the OECD reports that Korea’s fibre share exceeded 90 percent of fixed broadband subscriptions by end-2024. India should adapt that bundle, not the headline technology alone: fiber-first backhaul where density justifies it, plus superior user experience at transit, tourism, and public-service sites.

The lesson from entity ["organization","Anatel","brazil telecom regulator"]and the entity ["organization","Communications Authority of Kenya","kenya communications regulator"] is that small providers matter. Brazil's current planning documents explicitly note that small service providers play an important role in fiber expansion. Kenya, meanwhile, has developed a formal framework for community networks, a low-fee community network and service licence, and a Universal Service Fund strategy linked to 100,000 km of fiber, 25,000 public Wi-Fi hotspots, and 1,450 ICT hubs. India should adapt that lesson by treating PM-WANI not only as a public access programme but also as a local-provider market-making instrument—especially for PDOs, associations, cooperatives, self-help groups, and community institutions in underserved areas.

Make a Judgement

The most effective response is a **combined package**, not a single reform. The evidence points to five measures that should be prioritized together:

(i) open-access and lower-cost backhaul,
(ii) mandatory interoperability and simplified authentication,
(iii) municipal asset access with fast approvals,
(iv) a proportionate national security-and-trust baseline, and
(v) targeted—not universal—public support for commercially weak but socially important sites.

This package directly addresses the real supply-side bottlenecks identified in India's own consultation record: high upstream costs, last-mile fiber shortages, inconsistent user experience, operational fragmentation, and local execution barriers. It also avoids the two policy mistakes most likely to

slow deployment: adding new licensing burdens or relying only on broad subsidy without fixing operating economics.

This is the best consumer-first choice because it improves affordability, expands access in public-interest locations, raises reliability, and reduces the friction that makes Wi-Fi less attractive than mobile broadband. It is also the best competition-oriented choice because it makes room for small providers instead of only large nationwide operators. And it is the best technology-neutral choice because it does not prejudge whether the winning deployment architecture will be FTTH, shared fiber, Wi-Fi mesh, E-band/V-band backhaul, satellite support in remote areas, or mixed neutral-host systems; it instead focuses on outcomes—cost, coverage, security, interoperability, and quality. That is fully consistent with NDCP 2018, the Telecommunications Act 2023, and NBM 2.0's emphasis on universality, affordability, quality, infrastructure coordination, and meaningful connectivity.

In practical terms, TRAI should therefore recommend PM-WANI 2.0 as an execution package: preserve the light-touch authorization model, but add standardized wholesale backhaul offers, national roaming and identity standards, hotspot-quality benchmarks, public-asset access rules, and targeted DBN-linked viability support. That combination best balances innovation, competition, and consumer protection, while materially reducing friction for PDOs, PDOAs, ISPs, and venue owners.

Forward-Looking Implementation Plan

Short term, over the next 0–12 months. TRAI should finalize recommendations that: require published PM-WANI wholesale reference offers from ISPs/TSPs; define a common roaming and authentication profile;

recommend PM-WANI quality-of-service disclosure metrics for hotspot uptime, speed, and session success; and create a model municipal deployment protocol aligned with the RoW Rules 2024. The entity ["organization","Department of Telecommunications","india telecom dept"] should then notify corresponding amendments or guidelines, publish a national hotspot and asset inventory, and launch pilots in railway precincts, district hospitals, public libraries, and gram panchayat campuses. State governments and ULBs should nominate broadband nodal officers, identify hotspot-ready public assets, and enable corridor-based or bulk permissions rather than site-by-site approvals. ISPs and VNOs should publish standardized PDO products, while industry associations should create common implementation kits for MSME-scale PDOs.

Medium term, over the next 1–3 years. DoT and state governments should operationalize open-access use of BharatNet and state fiber for PM-WANI backhaul, especially in rural and semi-urban public institutions. TRAI and DoT should complete the next stage of spectrum reform by enabling lower-friction wireless backhaul in E-band/V-band and by testing shared-spectrum or AFC-style mechanisms where technically justified. PDOAs should migrate to standards-based, one-time onboarding and roaming, with Passpoint-compatible credentials and encrypted access as the default. State governments and ULBs should develop PPP deployment programmes for bus terminals, municipal markets, campuses, courts, and tourism zones, combining venue contribution, operator O&M, and targeted public support where needed. Startups and the PDO ecosystem should be brought into procurement frameworks through small-lot contracting, storefront deployments, and local maintenance partnerships rather than only large systems integrators.

Long term, over the next 3–5 years. India should move to nationwide interoperability across PM-WANI providers, with automatic onboarding, default roaming, and transparent quality benchmarking. Public Wi-Fi planning should also become more data-driven, using AI-assisted tools for channel planning, traffic prediction, preventive maintenance, and fault analytics where such tools reduce OPEX and improve service continuity. By this stage, India should also maintain an annual public benchmarking exercise against international leaders on hotspot density, venue coverage, authentication success, incident rates, and consumer outcomes, so that PM-WANI evolves as measurable digital infrastructure rather than a scheme counted only by installed hotspots.

Roles and accountability. TRAI should set the regulatory direction, market-design principles, and disclosure obligations. DoT should implement the framework, including PM-WANI technical standards, open-access backhaul rules, and spectrum or RoW coordination. ISPs and VNOs should provide transparent wholesale products, consumer-grade QoS where promised, and interoperable interfaces. State governments and ULBs should supply the public-space layer: permissions, asset inventories, and local PPPs. Industry associations should standardize templates, training, certification, and grievance pathways for smaller entrants. Startups, PDOs, PDOAs, and MSME operators should drive the distributed access layer and local maintenance model that PM-WANI was originally designed to unlock.

Monitoring, transparency, and consumer protection. The implementation framework should include a public dashboard reporting at least: live hotspots, geographic spread, hotspot uptime, median user throughput, time-to-install, complaint volumes, complaint-resolution timelines,

roaming success rates, and subsidy-linked performance where public support has been granted. Complaint handling should remain anchored at PDOA level, as already envisaged in PM-WANI, but with time-bound escalation and mandatory disclosure of grievance channels. Security monitoring should align with India's existing cyber-incident reporting and log-retention rules, while user notices should clearly state what data is collected, who the responsible entity is, and how complaints are resolved. This is essential if Public Wi-Fi is to be trusted as a complement to mobile broadband rather than seen as an inferior or risky fallback.

Q2. What are the major demand-side constraints limiting the uptake of Public Wi Fi services in the country? The limited uptake of public Wi-Fi services in India is not primarily a consequence of inadequate infrastructure deployment, but rather a manifestation of persistent demand-side constraints rooted in user behaviour, system design, and trust deficits. Although the country has witnessed significant growth in public Wi-Fi infrastructure under the PM-WANI framework—with lakhs of operational hotspots and millions of cumulative users—the level of sustained and habitual usage remains disproportionately low relative to policy ambition. This divergence clearly indicates that the challenge lies not in availability, but in adoption. Public Wi-Fi is not competing with a lack of connectivity; instead, it must compete with an already entrenched, affordable, and highly convenient mobile broadband ecosystem.

One of the most fundamental constraints arises from the dominance of mobile data services, which have reshaped consumer expectations around internet access. Ultra-low tariffs, coupled with seamless, always-on connectivity, have conditioned users to perceive internet usage as a near-

zero-cost and frictionless experience. Mobile broadband is pre-authenticated, continuously active, and deeply integrated into everyday digital behaviour. In contrast, public Wi-Fi often requires users to interrupt their ongoing activity, search for networks, complete multi-step authentication processes, and sometimes make separate payments. Even when public Wi-Fi offers a lower per-unit cost, the perceived inconvenience associated with switching outweighs the economic benefit. This creates a powerful behavioural lock-in, where users default to mobile data not because it is cheaper, but because it is easier.

Closely linked to this issue is the problem of authentication friction, which represents one of the most immediate and visible barriers to adoption. The current user journey under the PM-WANI ecosystem typically involves downloading an application, registering credentials, verifying identity through OTP, selecting a hotspot, choosing a data pack, and completing a transaction. Each of these steps, while individually manageable, cumulatively introduces a level of complexity that discourages users, especially in time-sensitive or low-attention environments such as transport hubs, marketplaces, or public offices. From a behavioural economics perspective, each additional step increases the likelihood of user dropout, reinforcing the tendency to remain on mobile data. The absence of persistent authentication further exacerbates this issue, as users are often required to repeat the process when reconnecting or moving between hotspots.

Another significant constraint is the lack of seamless roaming and session continuity across public Wi-Fi networks. Unlike cellular networks, which offer uninterrupted connectivity as users move geographically, public Wi-Fi

networks often function as isolated access points. Even within the same city, users may need to re-authenticate when switching between hotspots operated by different providers. This fragmentation undermines the perception of public Wi-Fi as a reliable and cohesive service. For a connectivity medium that is inherently location-dependent, the inability to ensure continuity transforms it into a sporadic, one-time utility rather than a habitual alternative. The absence of a unified identity layer or interoperable authentication framework prevents public Wi-Fi from achieving the network effect necessary for widespread adoption.

Equally important is the issue of trust, particularly in relation to security and privacy. Users frequently perceive public Wi-Fi networks as vulnerable, especially when managed by unfamiliar or small-scale operators. Concerns about data interception, identity theft, and financial fraud discourage users from engaging in sensitive activities such as online banking, digital payments, or accessing government services over public networks. This perception is reinforced by broader trends in cybercrime and the relatively low level of digital safety awareness among users. A significant proportion of the population lacks the confidence or capability to manage cyber risks, which further limits the scope of public Wi-Fi usage to low-value activities like casual browsing or entertainment. As a result, the perceived utility of public Wi-Fi remains narrow, reducing incentives for repeated use.

In addition to trust deficits, low awareness and poor discoverability of hotspots significantly constrain demand. Many users are either unaware of the existence of nearby public Wi-Fi networks or lack information about how to access them, their cost, or their reliability. Although the PM-WANI architecture includes provisions for hotspot discovery through app

providers, this functionality has not translated into a seamless and intuitive user experience. The absence of a unified discovery interface, standardized metadata, or a recognizable national identity for public Wi-Fi limits its visibility in everyday decision-making. A service that is not easily discoverable cannot be meaningfully chosen, and this invisibility directly suppresses adoption.

Digital literacy and capability gaps further compound these challenges, particularly in rural and semi-urban areas. A substantial segment of the population either lacks the skills required to use digital services effectively or does not perceive sufficient value in doing so. Even among those with basic internet access, the ability to perform tasks such as online transactions, document creation, or secure communication remains uneven. This lack of confidence translates into reluctance to experiment with new access modes like public Wi-Fi, especially when the perceived benefits are unclear. The problem is therefore not merely technological, but socio-behavioural, requiring interventions that go beyond infrastructure to address user readiness and perceived usefulness.

Taken together, these constraints reveal that the underutilization of public Wi-Fi in India is the result of an interconnected set of economic, behavioural, usability, trust, and capability barriers. Addressing these issues requires a shift in policy focus from supply-side expansion to demand-side optimization. The central objective should not be to make public Wi-Fi cheaper than mobile data, but to make it more convenient, trustworthy, and contextually valuable.

The most critical intervention in this regard is the implementation of frictionless authentication mechanisms that eliminate the need for repeated manual logins. A system based on one-time onboarding and persistent credentials would significantly reduce switching costs and align the user experience more closely with that of mobile broadband. Complementing this, the creation of a portable national Wi-Fi identity would enable seamless roaming across networks, transforming public Wi-Fi from a collection of isolated hotspots into a unified, federated access layer. Such an approach would ensure that user identity remains portable and not tied to a specific provider, thereby enhancing both convenience and competition.

Building user trust must be treated as a core policy priority rather than a secondary technical consideration. This requires the introduction of visible security assurance mechanisms, including standardized encryption practices, transparent privacy disclosures, and a recognizable certification framework for trusted hotspots. When safety becomes a clearly communicated feature rather than an implicit assumption, users are more likely to engage in higher-value activities over public networks, thereby increasing overall utility and adoption.

Improving discoverability is equally essential. A unified, map-based interface that provides real-time information about hotspot availability, pricing, quality, and security would reduce uncertainty and enable informed decision-making. Standardizing metadata and ensuring interoperability across applications would further enhance visibility and usability. In parallel, assisted onboarding and targeted digital literacy initiatives are necessary to bridge capability gaps, particularly among underserved

populations. These efforts should focus on practical, task-oriented training that demonstrates the real-world benefits of public Wi-Fi in areas such as education, healthcare, and digital governance.

While incentives such as free trial sessions can help overcome initial resistance, they should be used strategically to encourage first-time use rather than as a permanent subsidy model. Long-term sustainability depends on improving the underlying user experience rather than artificially lowering prices. Similarly, transparency measures such as quality-of-service dashboards and standardized grievance redress mechanisms can strengthen consumer confidence, although they function more as supporting tools than primary drivers of demand.

International experience reinforces these conclusions, demonstrating that successful public Wi-Fi ecosystems are characterized by seamless authentication, unified identity frameworks, strong security assurances, and effective discovery mechanisms. The common lesson across jurisdictions is that reducing user effort and making trust visible are far more impactful than expanding infrastructure alone. For India, the challenge is not to replicate foreign models, but to adapt these principles within the context of its own digital public infrastructure and user base.

Ultimately, the success of public Wi-Fi in India will depend on its ability to evolve from a technically available service into a compelling consumer product. This requires a coherent, consumer-centric framework that prioritizes ease of use, trust, interoperability, and meaningful utility. Without such a transformation, public Wi-Fi will remain an underutilized asset,

falling short of its potential to enhance digital inclusion and complement the broader broadband ecosystem.

Comments :

What are the major demand-side constraints limiting the uptake of Public Wi Fi services in the country?

Comments :

The limited uptake of public Wi-Fi services in India is not primarily a consequence of inadequate infrastructure deployment, but rather a manifestation of persistent demand-side constraints rooted in user behaviour, system design, and trust deficits. Although the country has witnessed significant growth in public Wi-Fi infrastructure under the PM-WANI framework—with lakhs of operational hotspots and millions of cumulative users—the level of sustained and habitual usage remains disproportionately low relative to policy ambition. This divergence clearly indicates that the challenge lies not in availability, but in adoption. Public Wi-Fi is not competing with a lack of connectivity; instead, it must compete with an already entrenched, affordable, and highly convenient mobile broadband ecosystem.

One of the most fundamental constraints arises from the dominance of mobile data services, which have reshaped consumer expectations around internet access. Ultra-low tariffs, coupled with seamless, always-on connectivity, have conditioned users to perceive internet usage as a near-zero-cost and frictionless experience. Mobile broadband is pre-authenticated, continuously active, and deeply integrated into everyday digital behaviour. In contrast, public Wi-Fi often requires users to interrupt

their ongoing activity, search for networks, complete multi-step authentication processes, and sometimes make separate payments. Even when public Wi-Fi offers a lower per-unit cost, the perceived inconvenience associated with switching outweighs the economic benefit. This creates a powerful behavioural lock-in, where users default to mobile data not because it is cheaper, but because it is easier.

Closely linked to this issue is the problem of authentication friction, which represents one of the most immediate and visible barriers to adoption. The current user journey under the PM-WANI ecosystem typically involves downloading an application, registering credentials, verifying identity through OTP, selecting a hotspot, choosing a data pack, and completing a transaction. Each of these steps, while individually manageable, cumulatively introduces a level of complexity that discourages users, especially in time-sensitive or low-attention environments such as transport hubs, marketplaces, or public offices. From a behavioural economics perspective, each additional step increases the likelihood of user dropout, reinforcing the tendency to remain on mobile data. The absence of persistent authentication further exacerbates this issue, as users are often required to repeat the process when reconnecting or moving between hotspots.

Another significant constraint is the lack of seamless roaming and session continuity across public Wi-Fi networks. Unlike cellular networks, which offer uninterrupted connectivity as users move geographically, public Wi-Fi networks often function as isolated access points. Even within the same city, users may need to re-authenticate when switching between hotspots operated by different providers. This fragmentation undermines the

perception of public Wi-Fi as a reliable and cohesive service. For a connectivity medium that is inherently location-dependent, the inability to ensure continuity transforms it into a sporadic, one-time utility rather than a habitual alternative. The absence of a unified identity layer or interoperable authentication framework prevents public Wi-Fi from achieving the network effect necessary for widespread adoption.

Equally important is the issue of trust, particularly in relation to security and privacy. Users frequently perceive public Wi-Fi networks as vulnerable, especially when managed by unfamiliar or small-scale operators. Concerns about data interception, identity theft, and financial fraud discourage users from engaging in sensitive activities such as online banking, digital payments, or accessing government services over public networks. This perception is reinforced by broader trends in cybercrime and the relatively low level of digital safety awareness among users. A significant proportion of the population lacks the confidence or capability to manage cyber risks, which further limits the scope of public Wi-Fi usage to low-value activities like casual browsing or entertainment. As a result, the perceived utility of public Wi-Fi remains narrow, reducing incentives for repeated use.

In addition to trust deficits, low awareness and poor discoverability of hotspots significantly constrain demand. Many users are either unaware of the existence of nearby public Wi-Fi networks or lack information about how to access them, their cost, or their reliability. Although the PM-WANI architecture includes provisions for hotspot discovery through app providers, this functionality has not translated into a seamless and intuitive user experience. The absence of a unified discovery interface, standardized metadata, or a recognizable national identity for public Wi-Fi limits its

visibility in everyday decision-making. A service that is not easily discoverable cannot be meaningfully chosen, and this invisibility directly suppresses adoption.

Digital literacy and capability gaps further compound these challenges, particularly in rural and semi-urban areas. A substantial segment of the population either lacks the skills required to use digital services effectively or does not perceive sufficient value in doing so. Even among those with basic internet access, the ability to perform tasks such as online transactions, document creation, or secure communication remains uneven. This lack of confidence translates into reluctance to experiment with new access modes like public Wi-Fi, especially when the perceived benefits are unclear. The problem is therefore not merely technological, but socio-behavioural, requiring interventions that go beyond infrastructure to address user readiness and perceived usefulness.

Taken together, these constraints reveal that the underutilization of public Wi-Fi in India is the result of an interconnected set of economic, behavioural, usability, trust, and capability barriers. Addressing these issues requires a shift in policy focus from supply-side expansion to demand-side optimization. The central objective should not be to make public Wi-Fi cheaper than mobile data, but to make it more convenient, trustworthy, and contextually valuable.

The most critical intervention in this regard is the implementation of frictionless authentication mechanisms that eliminate the need for repeated manual logins. A system based on one-time onboarding and persistent credentials would significantly reduce switching costs and align

the user experience more closely with that of mobile broadband. Complementing this, the creation of a portable national Wi-Fi identity would enable seamless roaming across networks, transforming public Wi-Fi from a collection of isolated hotspots into a unified, federated access layer. Such an approach would ensure that user identity remains portable and not tied to a specific provider, thereby enhancing both convenience and competition.

Building user trust must be treated as a core policy priority rather than a secondary technical consideration. This requires the introduction of visible security assurance mechanisms, including standardized encryption practices, transparent privacy disclosures, and a recognizable certification framework for trusted hotspots. When safety becomes a clearly communicated feature rather than an implicit assumption, users are more likely to engage in higher-value activities over public networks, thereby increasing overall utility and adoption.

Improving discoverability is equally essential. A unified, map-based interface that provides real-time information about hotspot availability, pricing, quality, and security would reduce uncertainty and enable informed decision-making. Standardizing metadata and ensuring interoperability across applications would further enhance visibility and usability. In parallel, assisted onboarding and targeted digital literacy initiatives are necessary to bridge capability gaps, particularly among underserved populations. These efforts should focus on practical, task-oriented training that demonstrates the real-world benefits of public Wi-Fi in areas such as education, healthcare, and digital governance.

While incentives such as free trial sessions can help overcome initial resistance, they should be used strategically to encourage first-time use rather than as a permanent subsidy model. Long-term sustainability depends on improving the underlying user experience rather than artificially lowering prices. Similarly, transparency measures such as quality-of-service dashboards and standardized grievance redress mechanisms can strengthen consumer confidence, although they function more as supporting tools than primary drivers of demand.

International experience reinforces these conclusions, demonstrating that successful public Wi-Fi ecosystems are characterized by seamless authentication, unified identity frameworks, strong security assurances, and effective discovery mechanisms. The common lesson across jurisdictions is that reducing user effort and making trust visible are far more impactful than expanding infrastructure alone. For India, the challenge is not to replicate foreign models, but to adapt these principles within the context of its own digital public infrastructure and user base.

Ultimately, the success of public Wi-Fi in India will depend on its ability to evolve from a technically available service into a compelling consumer product. This requires a coherent, consumer-centric framework that prioritizes ease of use, trust, interoperability, and meaningful utility. Without such a transformation, public Wi-Fi will remain an underutilized asset, falling short of its potential to enhance digital inclusion and complement the broader broadband ecosystem.

What targeted policy or regulatory measures may be required to address these demand-side constraints? Please provide your response in detail with justification.

Comments :

Comment on Targeted Demand-Side Measures for Public Wi-Fi Uptake in India

The policy implication is that India should not treat Public Wi-Fi as a cheaper clone of mobile data. It should instead redesign Public Wi-Fi as a frictionless, trusted, easy-to-find, interoperable, and situationally valuable access layer for high-footfall, high-density, low-income, public-service, and community contexts. The most effective package is a combination of: a federated National Wi-Fi ID with one-time onboarding and persistent credentials; Passpoint/OpenRoaming-compatible roaming and token-based or SIM-based reauthentication, with OTP only as a fallback; a PM-WANI trust mark built on encryption, privacy disclosures, and complaint redress; open hotspot discovery APIs integrated into mainstream apps; time-bound trial and voucher measures for first use and public-service use cases; digital literacy and assisted onboarding through Commons Service Centres and local institutions; and public QoS and grievance dashboards. This package is more consumer-first and more sustainable than permanent subsidies, because it addresses the real causes of abandonment: effort, uncertainty, distrust, and invisibility.

Demand-side problem definition:

Public Wi-Fi demand in India is constrained by a reinforcing set of behavioural, economic, awareness, trust, and usability barriers. TRAI's

consultation paper is clear that India is structurally mobile-first: users already rely on mobile data in public and on-the-move situations and shift to home/fixed Wi-Fi only where it is convenient or data-intensive. That means Public Wi-Fi is not competing with “no access”; it is competing with the consumer’s default habit of continuing on mobile data. In that context, even a small increase in login effort, uncertainty, or perceived risk can collapse willingness to switch. At the same time, Public Wi-Fi remains strategically important because TRAI also notes that future use cases such as AI, cloud services, immersive media, digital health, and connected devices will increase the value of high-capacity, low-cost access layers beyond mobile-only usage.

Demand-side constraint. What the evidence indicates? How it reduces uptake?

Mobile-first behaviour and low incremental value perception Consumers overwhelmingly use mobile data as the default access mode; mobile networks already satisfy most day-to-day needs, Public Wi-Fi feels optional rather than necessary, so even modest friction suppresses switching.

Authentication friction: Users often face app download, provider registration, OTP generation, login portal navigation, and small voucher purchase steps High abandonment, especially for casual, first-time, or low-literacy users.

Lack of seamless roaming: Moving between hotspots often requires repeat login and reauthentication. Public Wi-Fi feels episodic and fragile compared with mobile data’s continuity.

Security, privacy, and trust deficit: Users remain cautious about “open” networks, especially for financial or sensitive transactions. Public Wi-Fi is avoided for high-value use even when available and affordable.

Weak discovery and awareness: Many users do not know where hotspots exist, how to access them, or whether they are reliable. Hotspots remain underused because visibility and discoverability are poor.

Digital capability gap: A meaningful share of users lack confidence with online tasks and cyber-safety processes. Multi-step onboarding and trust judgments become disproportionately difficult.

Limited perceived utility: Public Wi-Fi is seldom bundled with clearly differentiated use cases such as large downloads, e-governance, telehealth, study, or commerce. Consumers do not see why Public Wi-Fi is worth the effort of connecting.

A further demand-side signal comes from household access patterns. Official survey data show that 13.7% of households still lacked internet access within household premises at the time of the CMS survey, yet among connected households almost all relied on mobile networks and only a relatively small minority used fixed/Wi-Fi access. That pattern suggests that even where consumers are online, familiarity with Wi-Fi as a routine access mode remains limited, especially outside homes, offices, airports, and railway environments. Public Wi-Fi therefore suffers not only from lack of awareness of individual hotspots, but also from weak habit formation at the population level.

The central regulatory conclusion, therefore, is that India does not have a single demand-side problem. **It has a stacked demand failure:**

(i) cheap and convenient mobile data reduces the incentive to try Public Wi-Fi;

(ii) clumsy onboarding raises switching costs;

(iii) lack of roaming undermines repeat use;

(iv) fear of fraud depresses trust;

(v) weak discovery keeps hotspots invisible; and

(vi) capability gaps magnify all of the above.

Demand-side policy should therefore be designed as a package, not as isolated interventions.

Targeted policy and regulatory measures:

1. The first and most important measure is a federated National Wi-Fi ID for PM-WANI and other compliant Public Wi-Fi systems. This should not mean a mandatory single app or a centralized consumer database. It should mean one-time consumer onboarding into an interoperable credential framework that can be accepted across PDOAs and hotspots. TRAI's own consultation explicitly identifies OTP dependence, legacy captive portals, fragmented payments, and lack of roaming federation as structural constraints, and it recalls TRAI's earlier "1-Click" architecture. The regulatory response should therefore be to require open federation standards for authentication and session portability. Consumers should be able to authenticate through any of several modes:

(i) app-based token,

(ii) device certificate,

(iii) Passpoint/Hotspot 2.0 profile,

(iv) SIM/eSIM-based method where supported, or

(v) OTP fallback where none of the above is available. That is both consumer-first and technology-neutral.

2. The second measure is a mandatory interoperability and roaming layer. TRAI should recommend, and the Department of Telecommunications", should notify, technical standards that make roaming a baseline expectation rather than an optional enhancement. The most appropriate approach is federated roaming modelled on Pass point/Open Roaming principles, while leaving implementation open to different commercial and technical routes. The goal is simple: once a user has authenticated on one compliant network, moving to another hotspot should not feel like starting over. This is where the National Wi-Fi ID and roaming mandate work together. Without roaming, the first-login problem becomes a repeat-login problem.

3. The third measure is a trust and security assurance framework. TRAI should recommend a “PM-WANI Trust Mark” for hotspots and apps that comply with a baseline consumer-protection standard: encrypted sessions wherever technically possible, certified PDOA/app software, clear privacy notices, data minimisation, simple consent language, visible complaint channels, incident response obligations, and transparent disclosure of price, speed, validity, and provider identity before purchase. India now has a more developed privacy framework, including the notified DPDP Rules, which emphasise clear and plain notices, specific purpose descriptions, and communication links for the data fiduciary. Public Wi-Fi should inherit those principles in a light-touch, proportionate way that does not overburden small PDOs. **The rule should be: trust must be legible to the user at the point of connection.**

4. The fourth measure is open discovery and awareness design. PM-WANI already envisages App Providers that can discover and display nearby hotspots, and official PM-WANI material notes that startups and wallet providers can become App Providers without licence fees. That is a major strength which should now be activated much more aggressively. TRAI should recommend that the Central Registry expose open APIs for real-time hotspot discovery, status, and basic quality metadata. Those APIs should be embeddable not only in PM-WANI apps but also in maps, travel apps, public transport apps, UPI apps, student-service apps, and local commerce platforms. Discovery should also move offline: common signage, QR-based connection prompts, multilingual instructions, and visibility in railway stations, bus depots, markets, schools, health facilities, and CSCs. A hotspot that consumers cannot find is functionally the same as a hotspot that does not exist.

5. **The fifth measure is targeted demand stimulation, but it should be designed narrowly and temporally.** Permanent consumer subsidies are not the right answer because they risk teaching users to treat Public Wi-Fi as a free commodity without improving repeat habit formation. A better approach is time-bound and use-case-bound support: first-session free trials; introductory data credits; student and job-seeker vouchers; telehealth and e-governance usage packs; merchant- or venue-sponsored sessions in markets, transit nodes, and public institutions. Official PM-WANI material already contemplates very small consumer coupon denominations—roughly ₹2 to ₹20 which makes low-cost, limited trials operationally feasible. The regulatory principle should be that trials are a behavioural nudge, not a permanent financial entitlement.

6. The sixth measure is digital literacy and assisted onboarding. India already has institutional channels for public internet access and digital inclusion under Digital India, especially the Common Service Centre network and the Public Internet Access Programme. These should be used to demonstrate how to locate, connect to, evaluate, and safely use Public Wi-Fi. Assisted onboarding matters because official skill indicators remain uneven. Consumers who are unsure whether a hotspot is genuine, whether a login page is safe, or whether a payment flow is legitimate are less likely to switch. A rural or semi-urban consumer-first strategy should therefore include hands-on onboarding, multilingual video explainers, and simple "safe Wi-Fi" advisories through schools, CSCs, self-help groups, local bodies, and public institutions.

7. The seventh measure is QoS transparency and grievance redress. Consumers should not have to guess whether a hotspot is worth using. TRAI should recommend mandatory ex ante display of plan validity, speed floor or expected range, session limits, fair-use terms, and refund policy. PDOAs should publish anonymised service-quality indicators—session success rate, median connection time, median throughput, complaint rates, and outage records—at least at city or district level. Each app or network landing page should provide a complaint escalation path with ticketing and time-bound closure. In behavioural terms, transparency reduces ambiguity; in regulatory terms, it converts Public Wi-Fi from an informal convenience into a measurable consumer service.

Finally, India should use the country's existing digital public infrastructure strengths instead of building a closed Wi-Fi silo. The entity organization, like "National Payments Corporation of India", "India retail payment's Unified

Payments Interface offers a widely adopted, consent-supported payment rail with “single click” features, while the entity "organization", "Open Network for Digital Commerce", "India ecommerce network" illustrates the value of interoperable open-network architecture rather than single-platform control. Public Wi-Fi can borrow those lessons without forcing a single dominant gatekeeper. In practical terms, that means open APIs, interoperable credentials, standard payment hooks, and non-discriminatory access for multiple apps, PDOAs, and MSME-facing service providers.

Evaluation of options

Two evaluation points matter most.

1. Frictionless authentication and roaming have the highest marginal impact because they directly target the point where consumers abandon the service today. TRAI’s consultation identifies OTP dependence, repeated logins, and lack of roaming as structural design failures, and international models show that once Wi-Fi becomes automatic and persistent, users stop treating it as a one-off chore.
2. Trust and discovery are complementary, not substitutes. A better map will not meaningfully raise adoption if consumers still distrust the network or expect a five-step login. Conversely, seamless login alone will not solve demand if users cannot find hotspots or cannot tell whether a service is safe.

On costs, India is well placed to adopt a proportionate approach. Official PM-WANI material suggests that a typical indoor PDO deployment may involve around ₹910 per month in indicative cost and an outdoor deployment around ₹1,475 per month, while coupon values can be very small and official illustrative revenue-sharing examples already

contemplate low-ticket retail models. That means demand-side reforms should be designed to avoid imposing new hardware costs on small providers whenever possible. Shared standards, centrally provided software templates, reference SDKs, certification reuse, and API-based federation are therefore preferable to venue-by-venue bespoke systems. TRAI's 2025 tariff intervention for PDO broadband, capping eligible FTTH connectivity charges to PDOs at not more than twice the comparable retail tariff, also reduces the risk that demand-side reforms will sit on top of an unsustainable cost stack.

The least attractive stand-alone option is a broad subsidy strategy without design reform. It may increase trial sessions, but it does not solve effort, trust, or continuity. If a user still must download an unfamiliar app, wait for an OTP, buy a micro voucher, and repeat the process later, a free pack will not create durable habit. For that reason, incentive measures should be adjuncts to the core architecture, not the architecture itself.

Recommended package:

The strongest recommendation is a combined package built around five pillars: federated identity, frictionless access, visible trust, open discovery, and transparent service quality. In practical terms, TRAI should recommend that DoT update the PM-WANI technical framework so that every compliant hotspot can support one-time onboarding, persistent credentials, federated roaming, and non-proprietary app interoperability. This should be paired with a PM-WANI Trust Mark and common disclosure template, a public hotspot registry and discovery API, a targeted first-use incentive layer, and mandatory QoS and complaint transparency.

This package is the best combination because it addresses the root causes of weak uptake rather than treating the symptoms. It lowers cognitive effort, reduces uncertainty, improves repeatability, and gives consumers a concrete reason to believe that Public Wi-Fi is safe, legitimate, and worth using. It is also friendlier to small providers than heavy ex ante regulation because the most important reforms are shared network and software standards, not recurring local compliance costs. The official PM-WANI model already permits broad participation by PDOs, PDOAs, and app providers without licence fees, entry fees, or net-worth barriers. The next policy step should therefore be to make that openness usable to consumers, not merely accessible to providers.

This recommendation is aligned with the policy logic of the National Digital Communications Policy, which explicitly sought to promote open public Wi-Fi through PDOAs and PDOs and targeted millions of hotspots as part of "Broadband for All." It is equally aligned with Digital India's goals of public internet access, digital inclusion, high-speed internet as a core utility, and universal digital literacy. Most importantly, it is consumer-first because it does not require a mandatory single app, a mandatory proprietary authentication method, or a mandatory Aadhaar-centric design. Technology neutrality is preserved by allowing multiple credential forms so long as they interoperate and meet minimum trust and privacy standards.

Three things should be avoided. First, India should not rely on permanent consumer subsidies as the main strategy. Second, it should not endorse mandatory app silos where each hotspot requires separate discovery and registration. Third, it should not continue to tolerate legacy captive-portal

dependence as the default national model. Those approaches may preserve formal openness but will not produce mass-market consumer uptake.

Implementation roadmap

A phased approach is both feasible and desirable because the required reforms are mostly standards, APIs, workflow redesign, and consumer communication—not a wholesale replacement of the underlying PM-WANI architecture. The initial emphasis should be on technical rules, pilots, consumer disclosure, and public visibility; the medium term should focus on deregulated federation and institutionalisation; the longer term should focus on optimisation, benchmarking, and continuous trust management.

Short term, over the first twelve months, TRAI should issue recommendations focused specifically on demand-side architecture: federated identity, persistent login, roaming, privacy notices, trust labels, and QoS disclosure norms. DoT should notify or endorse a reference standard stack for PM-WANI-compatible authentication, including token-based and Pass point-compatible methods, while preserving OTP as fallback. A common hotspot discovery API should be exposed from the Central Registry. Pilot deployments should be run in metros, railway stations, bus terminals, markets, universities, hospitals, and at least a few rural clusters through CSC-linked venues. Awareness campaigns should begin only where the new user journey is materially simpler than the current one.

Medium term, over one to three years, roaming federation should move from pilot to general obligation for compliant PDOAs; mainstream consumer apps should be allowed to integrate hotspot discovery and login under open and non-discriminatory rules; Trust Mark certification should become

visible at scale; digital literacy material should be embedded in CSC workflows, schools, and public institutions; and targeted vouchers should be limited to public-interest use cases such as education, telehealth, transit, migrant access, and employment services. By this stage, monitoring should shift from hotspot counts alone to actual demand metrics such as repeat-use rates, median time to connect, session success, complaint rates, and use in identified public-service categories.

Long term, over three to five years, India should aim for a mature interoperable public access layer: most compliant hotspots should support near-seamless reauthentication; quality data should inform AI-assisted hotspot placement and capacity planning; trust labels should be tied to auditable privacy and security performance; and India should benchmark its outcomes annually against federated and municipal models in Singapore, the EU, South Korea, Japan, Brazil, and Kenya. At that stage, the central policy question should no longer be “how many hotspots exist,” but “how many consumers use Public Wi-Fi repeatedly and confidently for meaningful digital activity.”

Stakeholder’s Core role in execution :

TRAI Recommend demand-side standards, disclosure rules, interoperability principles, QoS transparency, and consumer-protection safeguards.

DoT Notify technical framework changes, coordinate Central Registry APIs, establish certification pathways, and convene ecosystem pilots.

ISPs and VNOs Support interoperable back-end integration, bundled venue models, and roaming-compatible authentication where relevant.

State governments and ULBs should Provide public venues, signage, local awareness campaigns, and targeted use-case procurement in markets, transit, education, and health.

Industry associations : Build reference implementations, shared SDKs, and low-cost compliance templates for PDOAs and MSMEs.

Startups, PDOAs, and the PDO ecosystem: Build discovery tools, multilingual onboarding flows, trust-by-design interfaces, and last-mile customer support.

Monitoring and redress should be designed from the outset. Every certified network or app should provide complaint filing, status tracking, refund escalation, and a clear service provider identity. TRAI should encourage publication of a standard national dashboard with at least these indicators: active hotspots, successful sessions, median connection time, repeat-user share, roaming success, complaint closure time, refund rates, and serious security incidents. These data should be aggregated and privacy-preserving, but they should be public enough to build consumer confidence and regulatory discipline.

International practice and adaptation:

1. International experience demonstrates that **demand-side constraints in Public Wi-Fi—such as low user adoption, trust deficit, lack of awareness, and weak perceived value—are best addressed through user-centric policy frameworks rather than infrastructure expansion alone**.

Countries such as South Korea, the European Union, the United States, and Hong Kong have successfully increased Public Wi-Fi adoption by implementing measures focused on:

- **Affordability (free or low-cost access)**
- **Ease of use (frictionless authentication)**
- **Trust (security and privacy frameworks)**
- **Relevance (integration with public services and daily use cases)**

These interventions have transformed Public Wi-Fi into a **high-usage public digital utility**, rather than a passive connectivity option.

India can significantly enhance uptake under PM-WANI and related initiatives by adopting similar **demand-stimulation strategies aligned with global best practices**.

2. International Practices Addressing Demand-Side Constraints

2.1 European Union – Free, Uniform, and Trusted Access (WiFi4EU Model)

The EU's WiFi4EU initiative provides:

- **Free Public Wi-Fi in public spaces**
- **Simple login mechanisms (minimal friction)**
- **Uniform SSID and branding**
- **Minimum quality standards**
- **Public funding via vouchers for municipalities**

Impact:

- Over 90,000 hotspots deployed
- High adoption due to **zero-cost access + trust + simplicity**

Key Learning:

Demand increases when Public Wi-Fi is:

- Free at the point of use
- Easily discoverable and recognisable
- Reliable and secure

2.2 South Korea – Integrated Digital Ecosystem Approach

South Korea's model focuses on:

- **Free Wi-Fi in high-footfall public areas (transport, parks, public institutions)**
- **Seamless authentication and roaming**
- **AI-based cybersecurity systems**
- **Hotspot discovery applications**
- **Data-driven deployment based on user demand**
- **Continuous technology upgrades (Wi-Fi 6/7)**

Impact:

- Extremely high usage driven by **integration with digital lifestyle services**

Key Learning:

Demand is maximized when Wi-Fi:

- Is embedded in everyday digital services

- Provides seamless and uninterrupted connectivity
- Ensures strong user trust through security

2.3 United States & United Kingdom – Market-Driven Hybrid Model

These countries use:

- **Wi-Fi bundled with commercial services (retail, transport, hospitality)**
- **Carrier-grade Wi-Fi integrated with mobile networks**
- **Seamless roaming via Passpoint/Hotspot 2.0**
- **Venue-based incentives (free Wi-Fi attracts customers)**

Impact:

- High adoption through **commercial relevance and ecosystem integration**

Key Learning:

Demand rises when Public Wi-Fi:

- Complements mobile broadband
- Is embedded in consumer and business ecosystems

2.4 Hong Kong – Government-Led Unified Network Model

Key features:

- **Single government-backed Wi-Fi network (GovWiFi)**
- **Standardized authentication**
- **Wide coverage in public services and institutions**

Impact:

- High adoption due to **institutional trust and accessibility**

Key Learning:

Demand improves when Public Wi-Fi is:

- Positioned as a **public service entitlement**
- Integrated into governance infrastructure

3. Key Demand-Side Drivers Identified Globally

Across international models, the following **core drivers of Public Wi-Fi adoption** are consistently observed:

Driver	Explanation
Affordability	Free or low-cost access reduces entry barriers
Ease of Access	One-click login, no repeated authentication
Trust & Security	Strong encryption and privacy protections
Uniform Experience	Common SSID, predictable quality
Relevance of Use Cases	Integration with education, health, governance
Seamless Mobility	Roaming across hotspots
Awareness & Literacy	User education and digital literacy programs

4. Targeted Policy & Regulatory Measures for India (Based on International Adaptation)

4.1 Affordability & Access Measures

- Provide **free baseline Public Wi-Fi access** in essential public spaces (railways, hospitals, education hubs)
- Introduce **voucher-based or subsidized access models** for low-income users (EU model)

4.2 Frictionless Authentication Framework

- Transition from OTP-based login to:
  - **Auto-authentication (SIM-based / device-based)**
  - **Federated identity systems**
- Enable **single sign-on across all Public Wi-Fi networks**

4.3 National Unified Public Wi-Fi Identity

- Introduce a **common national SSID (e.g., "IndiaWiFi")**
- Standardize user experience across providers

4.4 Trust, Security, and Privacy Framework

- Mandatory compliance with:
  - WPA3 encryption
  - Secure authentication protocols
- Introduce a **"Certified Secure Public Wi-Fi" label**
- Strengthen data protection and privacy safeguards

4.5 Seamless Roaming & Interoperability

- Mandate interoperability across:
  - PM-WANI networks
  - Telco Wi-Fi networks
- Promote adoption of **Passpoint / Hotspot 2.0 standards**

4.6 Integration with Digital Public Infrastructure

- Link Public Wi-Fi with:
    - Digital India services
    - e-Governance platforms
    - Digital payments (UPI)
    - Telemedicine and e-learning

4.7 Awareness & Behavioural Interventions

- National campaigns promoting:
    - “Use Wi-Fi, Save Data”
- Digital literacy programs for rural and low-income users

4.8 Telco-Wi-Fi Convergence

- Encourage:
    - Bundled Wi-Fi access with mobile plans
    - Wi-Fi offloading strategies
- Enable operators to treat Wi-Fi as an **extension of mobile broadband**

4.9 Incentivisation of Usage

- Provide:
    - Free starter data packs
    - Usage-based incentives
- Promote **advertisement-supported free access models**

4.10 Data Transparency & QoS Assurance

- Public dashboards displaying:
    - Speed
    - Availability
    - Reliability
- Define **minimum QoS standards for Public Wi-Fi**

5. Conclusion

International experience clearly establishes that **Public Wi-Fi adoption is primarily a demand-side challenge, not merely a supply-side issue**.

Countries that have achieved high uptake have:

- Focused on **user experience, trust, and relevance**
- Treated Public Wi-Fi as a **core digital public infrastructure**
- Ensured **seamless, affordable, and secure access**

For India, the next phase of Public Wi-Fi proliferation must therefore shift from:

“Infrastructure creation” → “User adoption and meaningful usage”

By adopting targeted, consumer-centric regulatory measures aligned with global best practices, India can unlock the full potential of Public Wi-Fi as a **critical enabler of digital inclusion, economic growth, and next-generation connectivity**.

“Public Wi-Fi should be positioned not merely as a connectivity layer, but as a trusted, affordable, and seamlessly accessible digital public utility, supported by user-centric regulatory frameworks that actively stimulate demand and adoption.”

Q3. Despite the PM WANI initiative, scaling the number of public hotspots across diverse geographies, especially in remote and underserved regions, remains uneven. What are the key challenges in expanding both the density and geographic spread of hotspots, and what strategies could help accelerate more balanced, nationwide coverage? Please provide your response in detail with justification.

Comments :

Scaling Public Wi-Fi Hotspots: Challenges and Strategies for Nationwide Coverage :

Despite the success of PM-WANI in deploying hundreds of thousands of Wi-Fi hotspots, coverage remains heavily concentrated in a few urban centres. As of early 2026 there were 409,403 operational PM-WANI hotspots nationwide, but States like Delhi, Maharashtra, Karnataka and Uttar Pradesh account for the lion's share of deployments. Many remote and underserved regions – hilly, tribal or sparsely populated areas – still have little or no public Wi-Fi. This uneven rollout undermines Digital India objectives and leaves connectivity gaps where citizens need it most. The National Digital Communications Policy (2018) had targeted 10 million hotspots by 2022, but actual deployments (≈0.41 million) fell far short. In short, India's public Wi-Fi network has grown, but not yet in a balanced, geographically uniform way.

Several technical, economic and regulatory barriers explain this imbalance.

1. **Infrastructure and backhaul gaps pose a major challenge.** BharatNet and other fiber projects have laid hundreds of thousands of kilometres of fiber and connected over 2.18 lakh gram panchayats, but as TRAI notes, "overall fibre penetration at the last mile remains limited, particularly outside major urban centres". In practice, many villages lack any wireline or

even wireless backhaul; remote areas may rely on microwave links or expensive satellite/4G/LTE channels for backhaul. High costs and low competition make dedicated connectivity (leased lines or tower backhaul) unaffordable for small Wi-Fi providers. Moreover, reliable power supply is far from universal in rural areas. Even when fiber reaches a village, extending it to each hotspot is complex: maintaining ducts, running new cables, or coordinating with power companies. TRAI explicitly highlights the need to "streamline RoW processes and enable access to existing infrastructure such as street furniture, utility poles, ducts, and buildings" – and to ensure a reliable power supply via bulk billing – precisely to lower the cost and time of deploying new hotspots.

2. Commercial viability is weak in low-demand areas. In rural or low-traffic locations, a public Wi-Fi hotspot attracts only a handful of users per day. As the consultation notes, if local users "are unwilling to leave their mobile data connection, each hotspot attracts only a small number of paying customers". The average revenue per hotspot is therefore very low, often insufficient to cover recurring costs like backhaul bandwidth and electricity. This "lack of paying customers" problem dissuades entrepreneurs from setting up new PDOs (Public Data Offices) in thinly populated areas. Public Wi-Fi is a commodity business: without a clear revenue stream (e.g. fees, ads or bundled services), hotspots in remote hamlets or small towns simply are not economically sustainable. For example, TRAI's paper notes that digital literacy and awareness are uneven, so users may not see enough value to pay even low charges, further dampening demand. In short, market forces alone do not naturally incentivize building Wi-Fi networks in every village, without some subsidy or guaranteed patronage.

3. Policy and regulatory hurdles remain. By law, setting up a PDO or PDOA under PM-WANI requires some registration and compliance, which can deter informal or micro-entrepreneurs in rural areas. Rights-of-way for installing poles, cables and access points can be hard to obtain in practice, even after the Telecom Act 2023 introduced a single-window RoW portal (Gati Shakti) and mandated reasonable access rules. Inconsistent fee structures and slow approvals by state and municipal bodies still slow rollouts. On the positive side, PM-WANI permits even shopkeepers to become PDOs without a license, and uses deregulated spectrum for hotspots. But awareness of this ease-of-entry is low among small businesses. Finally, local coordination is often lacking: while fibre may exist, it lies unused without active projects (for instance, only 39 out of 100 Smart Cities have turned on free public Wi-Fi even though the fibre and ducts were largely in place). Similarly, many state-level schemes (e.g. Wi-Fi Choupal) deployed tens of thousands of rural hotspots, but "infrastructure issues" and "sustainability concerns" limited their impact.

Collectively, these factors – sparse backhaul, low ARPU, and deployment hurdles – explain why hotspot density remains uneven and sparse in India's hinterland. (For comparison, rural broadband targets in other countries often hinge on massive public investment or subsidies; without similar support, India's current model cannot by itself spur full rural coverage.)

To achieve balanced, nationwide public Wi-Fi coverage, targeted multi-pronged strategies are needed. These must combine infrastructure leverage, financial support, regulatory facilitation, and stakeholder engagement, always keeping citizens' needs and affordability in focus.

1. **Leverage national broadband infrastructure.** BharatNet and state fiber networks should form the backbone of rural Wi-Fi. The government and TRAI have recognized this: they recommend "use of BharatNet fibre as a common rural backhaul layer". In practice, each gram panchayat's BharatNet termination point can feed multiple Wi-Fi access points in the village. Programs like the BharatNet Udyami scheme empower local entrepreneurs to extend fiber from panchayats into villages. For example, Gujarat has used its Gujarat Fibre Grid Network to support public Wi-Fi in both rural clusters and urban public spaces. Replicating and expanding such state-led models – where the state helps aggregate and operate hotspots – can jump-start coverage. In fact, TRAI explicitly advises State Governments to act as PDOAs, aggregating Panchayats, CSCs, schools, health centres and other local entities under a single umbrella. A State-run PDOA can streamline onboarding (common registration portals, technical support, compliance help) and scale up deployments uniformly. The Gujarat case (a state-supported ISP functioning as PDOA) has shown that this model can accelerate hotspots across rural and urban areas.

2. **Expand funding and financial incentives.** Public support is essential to bridge the rural viability gap. The Digital Bharat Nidhi (DBN) – set up to finance broadband – can allocate grants or loans specifically for hotspot backhaul and equipment in remote areas. Indeed, TRAI proposes using DBN to fill last-mile gaps and has noted special loans: the SASCI (Special Assistance to States for Capital Investment)

scheme was recently amended (Mar 2026) to tie ₹4,000 crore of interest-free loans to states that implement the new Telecom RoW rules. Such financing reduces the cost barrier for installing towers, towerside Wi-Fi equipment, or ducts in villages. Similarly, viability gap funding (VGF) can be used to subsidize hotspots in very low-ARPU areas, recognizing these as public utilities with social returns. For example, free Wi-Fi deployments in 39 Smart Cities could have been encouraged by central grants; in India's context, a voucher or co-funding model (akin to the EU's WiFi4EU grants or USA's broadband subsidies) could be launched, where local governments or PDOs get grants to deploy and operate public Wi-Fi. These incentives should be larger in sparsely populated and high-cost regions (hilly areas, islands, J&K, North East, etc.), to level the playing field. In practice, funding could also take the form of lower backhaul tariffs (the June 2025 TRAI order already capped FTTH rates for PDOs at twice consumer rates), bulk power billing concessions, or property-tax relief for Wi-Fi installations. The goal is to make rural hotspot projects at least as attractive to entrepreneurs as building other infrastructure like telecom towers.

3. **Simplify and streamline deployment.** Regulatory and administrative processes should be optimized end-to-end. The recently notified Right-of-Way (RoW) rules (2024) are a step forward, but TRAI advocates taking it further: e.g., having district-level RoW committees (chaired by the District Magistrate with DoT, PWD and local bodies) to clear all installations. Local governments should be mandated to allow Wi-Fi access to streetlights, utility poles, bus shelters and public buildings without onerous fees. Faster, fixed timelines for RoW

approvals must be enforced. Also, given that backhaul competition is limited, policies should encourage shared infrastructure: multiple PDOs should be allowed to share fiber and ducts, and TSPs should be urged to offer wholesale bandwidth at low rates (as is already mandated). In urban contexts, Smart Cities should integrate Wi-Fi in their planning: for instance, Mumbai's MBBL and NBC codes could be updated to require malls, schools, hospitals and housing complexes to provision Wi-Fi zones. The idea is to "build Wi-Fi into the fabric of public infrastructure," so that when streets are dug for roads or fiber, conduit for Wi-Fi can be laid simultaneously, reducing extra cost. Bulk power supply arrangements (one connection feeding multiple APs, as TRAI suggests) can cut electricity costs.

4. **Engage and empower local actors.** Village-level and community actors should be at the heart of expansion. For rural areas, the existing network of Common Service Centres (CSCs) and village panchayats can be leveraged as Wi-Fi hubs. Under the Wi-Fi Choupal scheme, over 43,000 rural hotspots were installed by 2018 using CSCs and village entrepreneurs. Although that program faced sustainability issues, its model of combining BharatNet fiber, local operators (VLEs), and community Wi-Fi can be revived with better business support. New incentives to attract "Village Level Entrepreneurs" or small shops (kiranas, pharmacies, fair price shops) to act as PDOs in villages should be introduced: for example, micro-loans or equipment kits to set up a hotspot. In urban and peri-urban areas, local bodies and RWAs can recruit small businesses or individuals to host hotspots (as

PDOs) in markets, apartment complexes and co-working spaces. Municipalities should run awareness drives so citizens and entrepreneurs know how to join PM-WANI. They should also conduct "backhaul audits" to identify coverage gaps and use DBN funds to address them. Notably, TRAI suggests state government institutions themselves become PDOAs, aggregating hotspots from schools, health centres, and CSCs under one network. This both provides scale (a single login portal for many hotspots) and ensures maintenance and quality. In Gujarat, a state-supported ISP PDOA has demonstrated that this can bring tens of thousands of hotspots online efficiently. Similar models should be adopted by other states, especially those lagging in hotspot count.

5. **Adopt technology-neutral connectivity solutions.** Strategy must be flexible about technology. Where fiber is hard to deploy, wireless alternatives can be used. For instance, the government has already de-licensed 5.9–7.1 GHz and 57–66 GHz bands to support high-capacity Wi-Fi mesh backhaul. Satellite or high-altitude platforms could provide connectivity in extremely remote zones (India's Telecom Act now facilitates satellite services, which could carry Wi-Fi data to village gateways). Mobile carriers should be encouraged to integrate their networks with Wi-Fi: e.g., using LTE or 5G fixed-wireless access to feed Wi-Fi APs. The Wireless Broadband Alliance notes that deploying a simple outdoor Wi-Fi hotspot (with solar power and a small antenna) costs roughly **$2,500**, versus ~$50,000 for a cellular tower in remote areas. Indian carriers can exploit this cost

advantage by offloading rural broadband traffic to Wi-Fi. Similarly, emerging standards (Pass point/Hotspot 2.0) and expansion of the 6 GHz band can make roaming seamless and enhance capacity. Ensuring tech-neutral rules (e.g. allowing use of unlicensed spectrum and small-cell repeaters) will enable innovative rural broadband architectures without favouring one vendor or operator.

6. **Align with legal mandates and standards.** All of the above strategies must be integrated with India's policy framework. The NDCP-2018 and Digital India vision emphasize "Broadband for All" and inclusive growth, which inherently includes underserved regions. TRAI's 2023 Telecom Act and 2024 Right-of-Way rules already provide tools for faster broadband rollout; these should be fully operationalized and extended to cover Wi-Fi facilities explicitly. Key standards (e.g. IEEE 802.11ac/ax/ax and WPA3 security) should be mandated for all public Wi-Fi gear to ensure uniform performance and safety. Regulatory frameworks like the Digital Bharat Nidhi and Universal Service Obligation Fund (USOF) should explicitly include public Wi-Fi as a covered intervention. For example, the broadband USOF already funded Wi-Fi at BSNL rural exchanges and Gram Panchayats; this can be expanded under BharatNet Phase-III as "Wi-Fi hotspots in every village, to be funded by USOF/DBN".

International practices provide useful analogies.

The EU's WiFi4EU program, for example, distributed grants to thousands of municipalities to create free hotspots, recognizing that local funding can spur usage. Likewise, the US's Rural Digital Opportunity Fund allocates

subsidies to operators serving high-cost rural areas. India can adapt such models: for instance, offering competitive grants for local bodies to deploy Wi-Fi in backward regions. The Wireless Broadband Alliance's rural Wi-Fi report highlights how hybrid networks (fiber to a village plus local Wi-Fi mesh) can cover hard terrain, and notes that Wi-Fi-based fixed wireless can deliver gigabit speeds over short distances. Taking inspiration, PM-WANI could allow (and encourage) local mesh-network trials in hilly areas, supported by incentives.

In summary, addressing supply-side constraints requires a holistic, consumer-centric approach. Policy must treat public Wi-Fi as a critical digital utility:

- ✓ Infrastructure should be shared and coordinated (fiber, power, poles).
- ✓ Financing should target the toughest areas (DBN, VGF, loans for RoW compliance).
- ✓ Regulation should remove friction (permit by default, standardize processes).
- ✓ Community actors (states, municipalities, entrepreneurs) must be empowered to lead deployments.

Combining these measures will not only expand hotspot density and reach, but also ensure that every citizen, urban or rural, can access affordable high-speed internet over public Wi-Fi. This forward-looking strategy is aligned with India's broadband laws (NDCP 2018, Digital Communications Act 2023) and international best practices, and it directly benefits consumers by delivering inclusive and resilient connectivity across the nation.

Q4. What changes, if any, are required in the existing PM-WANI framework to improve revenue certainty and long-term sustainability for PDOs/PDOAs? Please provide your response in detail with justification.

Comments :

1. Advancement of Technology

Emerging Wi-Fi technologies can dramatically lower operating costs for PDOs/PDOAs and improve network efficiency. Next-generation standards like Wi-Fi 6/6E (802.11ax) and the forthcoming Wi-Fi 7 (802.11be) offer multi-gigabit speeds, greater spectral efficiency, and advanced features such as MU-MIMO and OFDMA. As TRAI notes, the evolution to Wi-Fi 6/6E "has significantly enhanced the capacity, efficiency, and performance of unlicensed wireless networks". These improvements mean each hotspot can serve many more users without additional hardware, reducing the number of access points needed. In fact, government reforms have de-licensed the 6 GHz band for low-power use, giving PDOs access to up to 1.2 GHz of new spectrum. This larger clean spectrum enables wider channels (e.g. 160 MHz) and less interference, which can support high-throughput services with lower latency. In practice, adopting Wi-Fi 6/6E (and future Wi-Fi 7) access points will cut per-unit data costs for PDOs by allowing more clients per AP and by offloading greater traffic from expensive mobile spectrum.

Open and cloud-based Wi-Fi architectures further strengthen PM-WANI. For example, the Telecom Infra Project's OpenWiFi initiative (supported by TIP members like HFCL) disaggregates hardware and software. HFCL demonstrated that OpenWiFi access points achieve the same performance as proprietary equipment while slashing development costs. Because the

software is open source, development expenses are shared among vendors, lowering end-user prices. IO Networks (HFCL) is already rolling out low-cost OpenWiFi APs (including 802.11ax/Wi-Fi 6 devices) for rural PM-WANI deployments. We recommend that PM-WANI actively endorse open, multi-vendor solutions (via specifications or conformity schemes) so that PDOs can source affordable equipment from multiple suppliers.

Cloud-based AAA and management systems also reduce opex. In a traditional setup, each PDO might need dedicated RADIUS/AAA servers; moving these services to a shared cloud platform lowers per-hotspot costs and simplifies maintenance. Similarly, automated onboarding mechanisms (e.g. device auto-configuration, QR-code login) can eliminate laborious manual steps. For instance, global standards like IEEE 802.11u/Hotspot 2.0 (Passpoint) allow devices to automatically authenticate to Wi-Fi without repeated logins. We urge PM-WANI to adopt Passpoint-compatible certifications for PDO hardware and devices, enabling users' devices to join any compliant hotspot seamlessly. This would shrink user friction (and thus increase usage), while reducing the need for human support.

New backhaul methods can also enhance sustainability. "Shared backhaul" – for example, allowing PDOs to interconnect via city or community fiber rings – can spread the cost of high-speed backhaul across many hotspots. As the Minister of State (Telecom) recently observed, enabling each storefront PDO to "access fibre-to-the-home connections" and building a "shared backhaul linking isolated digital nodes into a harmonious network" are key to nationwide coverage. In practice, this could mean policy support for multiple PDOs in a cluster to lease one fiber link cooperatively, or preferential access to BharatNet/BharatNet Udyami networks.

Cloud-managed Wi-Fi mesh nodes (powered by Wi-Fi 6E) could further expand coverage with minimal power/latency penalties. Collectively, these technology upgrades lower per-hotspot opex (through economies of scale and hardware efficiency) and make revenue streams more predictable for aggregators and operators.

2. Alignment with Laws & Standards

The PM-WANI framework was deliberately designed as a lightly regulated model, and this principle should be preserved. Crucially, PDOs and PDOAs remain *licence-exempt* under current rules. TRAI explicitly notes that "PDOs are not required to obtain a telecom licence, which significantly lowers compliance burdens", and that PDOAs/App Providers operate under a "licence-exempt, registration-based" regime. Any changes to PM-WANI should maintain this ease of entry – small businesses should not be saddled with new licensing or fee requirements. Instead, regulatory updates should clarify grey areas: for instance, explicitly confirming that PDOAs are not subject to Internet Service Provider (ISP) licencing, and defining whether PDOAs may own the last-mile backhaul (e.g. fibre).

Compliance with national laws and security standards must be reinforced. PM-WANI must remain consistent with the Telecom Act, IT Act, and Data Protection legislation. In particular, as the new Digital Personal Data Protection Act (DPDP Act) takes effect, PDOAs and App Providers will be categorized as data fiduciaries. Clear guidance is needed on data handling (e.g. consent for storing voucher purchases, tokenization of personal data, retention limits). We recommend mandating privacy notices for users and requiring PDOAs to implement reasonable security measures (e.g. encryption on the Ethernet leg, WPA3 on Wi-Fi, regular audits). This aligns

with TRAI's view that, under compliant operation, a Wi-Fi network "can offer secure, reliable, and interoperable broadband access" at carrier-grade quality. For cybersecurity, PM-WANI devices should follow Government of India cybersecurity guidelines (e.g. CERT-IN best practices) and any IoT/Device security standards. We also suggest a public registry of certified Wi-Fi equipment (analogous to CDOT's UASL guidelines) to assure PDOs that any approved AP hardware meets Indian specifications.

Spectrum allocation and usage rights should be unambiguous. The Government has already delicensed key bands for Wi-Fi (2.4/5/6 GHz) to encourage deployment. Going forward, regulators should ensure that any new Wi-Fi spectrum (e.g. future 7 GHz allocations) is promptly opened for PM-WANI use. Additionally, DoT or TRAI could issue a consolidated FAQ or circular stating that PM-WANI operations do not require traditional spectrum licences, which would eliminate any lingering confusion for entrepreneurs.

3. Forward-Looking Regulatory Approach

To scale sustainably, PM-WANI must include built-in incentives and protections that balance PDO profitability with consumer value. One example is the 71st Tariff Amendment Order (2025) already implemented by TRAI, which caps TSP backhaul charges to PDOs at twice the standard FTTH tariff. This rule prevents arbitrary price hikes by backbone providers and gives PDOs predictable costs. We recommend extending similar caps or priority access to other backhaul modes (e.g. leased microwave, satellite) to ensure rural PDOs are not disadvantaged.

Establishing minimum Quality of Service (QoS) standards will also raise the overall viability of hotspots. For instance, TRAI can define service targets (e.g. minimum Mbps per user, latency thresholds) that PDOAs must meet

across their network. Technical frameworks like IEEE 802.11e/WMM (Wi-Fi Multimedia) already allow networks to prioritize latency-sensitive traffic. We suggest incorporating such standards into PM-WANI guidelines: compliance could be monitored via periodic speed tests or app analytics. PDOAs that consistently meet QoS benchmarks could be granted premium status or branding, incentivizing good service.

Power supply and other inputs should be made as seamless as possible. The consultation paper highlights the benefits of bulk electricity connections, where multiple hotspots share a single utility meter. We endorse this: municipalities or electricity regulators should allow a group of Wi-Fi APs (within a market or neighborhood) to register as one customer for billing, drastically reducing installation and billing hassles. Similarly, Right-of-Way (RoW) rules should be actively harmonized: the 2024 RoW Rules already ease deployment on poles and ducts, but implementation must be monitored at the state/district level to avoid local delays.

Standardized Service Level Agreements (SLAs) and multi-party accountability are also needed. For example, any rooftop or public-area owner hosting a PDO might sign an SLA with the PDOA guaranteeing site access, power provision, and basic maintenance. Local governments (City Wi-Fi projects, Smart City SPVs) can play a coordinating role by co-signing agreements that lay out responsibilities for fiber uptime, power, and security. This reduces operational uncertainty for PDOAs. In sum, by enforcing fair cost frameworks (tariffs, power) and setting clear technical benchmarks (QoS, uptime), the regulator can create an environment where investing in Wi-Fi hotspots is a reliable business decision.

4. Consumer-First Orientation, Transparency & Protection

Stabilizing PDO/PDOA economics ultimately benefits consumers. When network providers have predictable revenue, they can maintain equipment, ensure uptime, and even subsidize initial usage – improving the user experience. For instance, a PDO that is confident about covering its costs may offer free Wi-Fi trial periods or low subscription rates. This in turn raises user adoption. By contrast, the consultation paper shows that unpredictable micro-transaction revenue currently deters both PDOs and users: "mobile data provides a seamless, always-on experience" while Wi-Fi demands extra steps. Removing these hassles (as recommended in Pillar 1) will thus increase usage, generating more income per hotspot and closing the viability loop for providers.

Transparency is key to building trust. We urge TRAI to require PDOAs to publish basic performance and pricing information. Possible measures include: a public dashboard (or app) displaying average speeds and uptime for each PDO's hotspots; standardized tariff cards or menus at each location; and easy-to-find contact info for customer service. Just as mobile tariffs are regulated to be published, a similar practice for Wi-Fi vouchers would reassure customers. Moreover, branding mechanisms (e.g. a "Certified Secure Wi-Fi" label for compliant hotspots) can signal to users that connectivity is safe. To protect consumer interests, the PM-WANI grievance framework should be strengthened: PDOAs must have a defined escalation path (and be held to response timelines) for customer complaints, analogous to telecom ombudsman rules.

In short, policies that ensure PDOs can survive economically directly translate to better service for end-users – more hotspots, fewer outages, and lower prices. As TRAI notes, when Wi-Fi is "properly designed, securely

configured…[and] integrated with strong authentication and encryption," it offers a high-quality, trusted connectivity option. Maintaining this consumer-first focus in regulatory changes will guarantee that revenue certainty yields tangible benefits for subscribers.

5. Practical Implementation

The above reforms must be paired with on-the-ground incentives and feasible steps. We recommend piloting cluster models: for example, appoint one state-sponsored PDOA (such as a public ISP or municipal IT department) to serve all PDOs in a rural block or urban ward. This "aggregator" would handle procurement, billing, and tech support, while local shopkeepers or schools act as the front-end PDOs. Such models (e.g. Gujarat's state-anchored PDOA) have already shown success in onboarding many hotspots at low cost.

Financial incentives can jumpstart growth. The government could offer capital subsidies or low-interest loans to PDOAs for initial equipment (access points, antennas) through existing schemes (e.g. under Universal Service Obligation Fund). Bulk purchasing by aggregators would reduce per-unit costs of APs and routers. On the revenue side, PDOAs should be allowed to diversify income (subject to fair-use rules) – for instance, by offering advertising on captive portals or providing analytic services to local businesses.

Shared infrastructure is also crucial. Operators should be encouraged to roll out neutral-host networks in large venues (markets, housing complexes, transit hubs), where multiple PDOs can co-locate antennas on a common backhaul. Similarly, encouraging aggregators to partner with schools, hospitals, and panchayats (by providing free Wi-Fi equipment in exchange

for space and power access) will minimize capex for PDOs. Risk-mitigation tools can include bandwidth reservation agreements with TSPs (e.g. guaranteed rates from TSPs during peak hours) and fast replacement warranties for hardware.

In every case, implementation should be low-cost and incremental. Existing digital public infrastructures like CSCs and post offices can be upgraded as PDOs; municipal IT cells can serve as PDOAs. By leveraging these already-available assets, the PM-WANI expansion becomes an evolution rather than a greenfield build.

6. International Implementation & Best Practices

Globally, successful public Wi-Fi systems emphasize seamless, affordable access and multi-stakeholder models – lessons India can adapt. Singapore's Wireless@SGx network, for example, provides free Wi-Fi at thousands of hotspots with a single unified login (via a smartphone app) and Roaming and Federation standards. Users automatically connect in many locations without re-authentication. Similarly, the EU's WiFi4EU initiative has funded over 90,000 municipal hotspots across Europe, all free to the public under a common SSID, demonstrating that completely free access drives mass adoption.

In the US and EU, mobile carriers often offload data to Wi-Fi using Passpoint/Hotspot 2.0 and **OpenRoaming** technologies. The TRAI consultation itself highlights that "globally available contemporary authentication methodologies such as Passpoint (Hotspot 2.0) eliminate manual login". Embracing these standards in PM-WANI would mirror international practice and allow devices to move between cellular and Wi-Fi networks seamlessly.

Japan and South Korea have densely deployed public Wi-Fi (with strong operator involvement and integrated digital services), showing the importance of government backing and universal access. Brazil's **Wi-Fi Brasil** program is a notable example in the Global South: by 2022 it had installed over 15,000 public access points in vulnerable communities (66% of them in schools and health clinics). This demonstrates that targeted public investment and partnerships with local institutions can rapidly expand coverage. Community-driven networks (such as Kenya's mesh clusters or Spain's Guifi.net) further illustrate that grassroots cooperatives can thrive when supported by simple regulation.

In summary, international models reinforce that a combination of free/basic access, unified user experience, robust security, and multi-stakeholder deployment is key. India should adopt relevant elements – for instance, an "IndiaWiFi" common SSID (like EU's WiFi4EU), integration with UPI or Aadhaar for frictionless logins (inspired by Singapore's app), and encouragement of neutral-host or municipal networks (as in many US cities). Alignment with global roaming consortia (WBA's Open Roaming) would also put India's network on par with best practices.

Recommendation: In light of the above, we recommend that TRAI and DoT implement a comprehensive, user-centric upgrade of PM-WANI. Key changes should include: endorsing modern technologies (Wi-Fi 6/7 hardware, TIP OpenWiFi APs, cloud AAA and Passpoint/QR login) to cut costs and friction; codifying license-exempt status while enforcing security and data protection standards for consumer trust; mandating fair backhaul pricing and power arrangements to stabilize PDO economics; and

enhancing transparency (public QoS data, clear tariffs, grievance channels) for accountability. These measures – aligned with NDCP-2018's goals of affordable, ubiquitous broadband – will ensure PDOs/PDOAs can achieve reliable revenue and scale, which in turn guarantees affordable, high-quality Wi-Fi services for every Indian consumer.

Q5. Are there any other challenges currently faced by PDOAs/PDOs? If yes, what changes can enhance the participation of entrepreneurs under the PM-WANI framework? Please provide your response in detail with justification.

Comments :

1. Define the problem

India's public Wi-Fi initiative (PM-WANI) targets ubiquitous, affordable connectivity in line with NDCP-2018's vision of ubiquitous digital infrastructure[1]. Yet uptake has been far below goals: only ~0.4 million hotspots exist vs. the 10 million envisioned by 2022[2]. Key challenges undermine PDOA/PDO viability and growth:

- **Weak revenue models & low profitability:** PDOAs/PDOs struggle to earn predictable income. TRAI notes *"lack of predictable revenue streams…low tariffs, and absence of complementary monetization options (ads, bundling)"*. Many PDOAs report stocked access points and negligible returns. High fixed costs (equipment, power, backhaul) against few paying users make break-even unlikely under current pricing.
- **High operating costs (backhaul, equipment):** Securing affordable last-mile backhaul is a bottleneck. ISPs/TSPs often insist on expensive

dedicated links (ILL), which can cost 40–80× more than consumer fiber plans[5]. This drives annual broadband bills for a PDO into lakhs, destroying margins. Even with the DoT Tariff Order capping PDO broadband rates, many operators find costs prohibitive.

- **Complex onboarding and compliance:** Despite being licence-exempt, setting up a PDO/PDOA involves multi-step registration, device configuration, and KYC obligations. The legacy DoT OTP rule (from 2009) still applies, forcing users through SMS logins and voucher purchases. Interoperability gaps mean apps and PDOs from different providers may not work together[8]. Regulatory and multi-agency approvals (municipal permits, RoW, power connections) further burden small entrepreneurs.
- **Awareness and demand shortfall:** Low public awareness stifles both supply and demand. Many shopkeepers and rural entrepreneurs don't realize they can become PDOs without a license, so few register. Likewise, end-users seldom know where PM-WANI hotspots exist or how to access them. As of late-2024 only ~1.8 million users had ever connected, consuming just 58.5 PB of data nationwide – a tiny fraction of the potential user base.
- **Competition with cheap mobile data:** Generous 4G/5G data plans (≈₹7.9/GB) have conditioned consumers to expect "nearly free" connectivity. This makes paid Wi-Fi vouchers less attractive. Incumbent telcos also see PDOAs as a threat and have lobbied to keep PM-WANI unprofitable.
- **Trust, security and digital literacy:** Users often distrust open Wi-Fi for transactions, preferring familiar mobile networks. Concerns about data privacy or service reliability further depress adoption. Technical and

literacy gaps (unreliable power/backhaul in rural areas) also limit service quality.

These challenges together erode :

(a) PDOA/PDO revenue sustainability and business viability,

(b) the incentive for new entrepreneurs to enter the scheme, and

(c) consumer coverage, affordability and trust. Uncertain revenues and slim margins make existing PDOs vulnerable (many report breaking even only with dozens of daily users. Prospective entrepreneurs hesitate to invest in infrastructure that may never pay off. Meanwhile, consumers in underserved areas face sparse, unreliable Wi-Fi options and often end up paying more for mobile data or going online less – undermining PM-WANI's inclusion goals.

2. Possible solutions:

A broad suite of interventions can address these challenges:

- **Regulatory and policy reforms:** Enforce tariff parity so PDOs pay rates similar to retail broadband (as TRAI's 71st Order intended[6]). Streamline approvals by establishing single-window RoW and bulk-power rules. Clarify roles (e.g. let State agencies/CSCs serve as PDOAs).
- **Financial incentives and viability support:** Provide targeted subsidies or viability-gap funding (e.g. via Digital Bharat Nidhi or USOF grants) to offset low initial returns. Tax or fee waivers for equipment and power can lower entry costs. Encourage CSR-funded and public-private schemes (e.g. funding Wi-Fi in anganwadis or health centres) to expand reach.
- **Simplified onboarding & authentication:** Replace burdensome OTP portals with one-click authentication. For example, adopt Passpoint

(Hotspot 2.0) and integrate UPI/Aadhaar e-KYC for auto-login. Certify and standardize PM-WANI apps/devices to ensure true plug-and-play interoperability. This reduces technical friction for small shopkeepers and users.

- **Standardized revenue-sharing and monetization:** Develop model revenue frameworks (e.g. clear 80/20 PDO/PDOA splits) to set expectations. Enable diverse revenue streams: paid access in premium venues, freemium in public hubs, ad-funded or bundled plans (with TSPs). For example, allow local businesses to sell advertising on login pages or aggregate footfall data for retail analytics. Institutional "anchor" clients (schools, panchayats) could bulk-purchase Wi-Fi, guaranteeing baseline demand.
- **Awareness-building and capacity development:** Launch nationwide campaigns to educate entrepreneurs and consumers about PM-WANI benefits (no license needed, supplementary income, etc.). Use digital literacy drives (via NGOs, schools, SHGs) to teach people how to use hotspots safely. Train entrepreneurs (shopkeepers, self-help groups) in hotspot setup/management via existing rural infrastructure (e.g. CSCs, Krishi Vigyan Kendras).
- **Integration with other schemes and venues:** Leverage government assets and programs: e.g. equip CSCs, railway stations, bus stands, hospitals and tourism sites as PDO hotspots. Involve local bodies by allowing municipal Wi-Fi (streetlights, parks) to join PM-WANI. Encourage BharatNet Udyami entrepreneurs to extend fiber to PDOs as part of the last-mile network.
- **Technology enablers:** Promote open-standard hardware (e.g. TIP OpenWiFi-compliant APs) to reduce costs and ensure multi-vendor compatibility. Use cloud-based AAA platforms (so small PDOs need no on-

site server). Deploy data analytics (demand forecasting, GIS mapping) to guide hotspot placement in high-need areas. Share existing backhaul (BharatNet fiber, FTTx) and power infrastructures to cut PDO connectivity costs.

Each of these interventions tackles specific challenges: for example, subsidies or VGF directly improve:

(a) revenue prospects and make it worthwhile for entrepreneurs, while one-click authentication

(b) lowers technical barriers to entry. Diversifying revenue (ads, bundling) creates new income streams for PDOAs/PDOs, reducing reliance on user fees. Broad awareness campaigns and partnerships expand the pool of willing PDOs and help build user trust. Taken together, these measures reinforce the PM-WANI ecosystem's sustainability.

3. Evaluation of the options:

Below is a high-level comparison of key solution categories against the criteria:

- **Tariff & infrastructure reforms (e.g. price cap, shared backhaul):**
- *Consumer benefit:* High – lowers costs for end-users via cheaper Wi-Fi rates.
- *Ease:* Moderate – requires regulatory orders and coordination with ISPs/TSPs.
- *Cost:* Low direct fiscal cost; potential revenue impact for incumbents (resistance risk).
- *Scalability:* Nationally scalable once rules are set.

- *Alignment:* Strong – furthers NDCP-2018 goals of affordable ubiquitous broadband.
- *Risks:* Telco pushback; needs enforcement (some operators already sought to overcharge PDOs).

- **Simplified onboarding & auth (Pass point, eKYC):**

- *Consumer benefit:* High – seamless Wi-Fi logins boost uptake and trust.
- *Ease:* Moderate–high – requires tech integration (app updates, possibly device upgrades) but leverages existing standards.
- *Cost:* Low to moderate – development of common gateway/standards; one-time tech investment.
- *Scalability:* High – standard solutions work nationwide.
- *Alignment:* High – directly addresses inclusion by making access user-friendly (as TRAI consultation notes).
- *Risks:* Initial complexity in rollout; small PDOs may need support to install compliant APs.

- **Financial incentives (subsidies, VGF, CSR):**

- *Consumer benefit:* Indirect – by ensuring service availability in low-income or remote areas.
- *Ease:* Moderate – requires budget allocation and transparent disbursement mechanisms (e.g. DBN funds).
- *Cost:* Budgetary outlay – but can be ring-fenced (e.g. from USOF).
- *Scalability:* Conditional – effective if well-targeted; limited by available funds.
- *Alignment:* High – supports NDCP's universal access targets.

- *Risks:* Potential misuse or mis-targeting of funds; must guard against gaming the system.

- **Awareness and training programs:**

- *Consumer benefit:* High long-term – more people learn about and trust public Wi-Fi.
- *Ease:* Moderate – leverages existing channels (schools, panchayats, CSR).
- *Cost:* Low to moderate (campaign materials, training sessions).
- *Scalability:* High – can be rolled out nationwide via digital media, Gram Sabhas, etc..
- *Alignment:* Strong – fosters digital inclusion and entrepreneurship (NDCP mandate).
- *Risks:* Slow payoff (behaviour change takes time); requires sustained effort.

- **Integration with public institutions (CSCs, smart cities):**

- *Consumer benefit:* High – expands hotspot network in key locations (e.g. CSCs in every village).
- *Ease:* Moderate – depends on inter-department coordination (e.g. DoT with States/ULBs).
- *Cost:* Relatively low (using existing assets); possible small capex for APs.
- *Scalability:* High potential (CSCs and ULBs exist nationwide).
- *Alignment:* High – builds on Digital India infrastructure, aligns with smart city goals.
- *Risks:* Institutional inertia; must clarify roles so entities don't "pass the buck".

- **Technology enablers (Open WIFI, analytics):**

- *Consumer benefit:* Medium – improves reliability/interoperability, which builds trust.
- *Ease:* Moderate – requires industry adoption of standards (e.g. HFCL's Open WIFI APs).
- *Cost:* Variable – can reduce long-term costs but needs initial R&D/standards work.
- *Scalability:* High in urban/enterprise contexts; rural deployment depends on basic infrastructure.
- *Alignment:* Good – consistent with NDCP's push for innovation and spectrum reforms.
- *Risks:* Market fragmentation if too many standards; need common certification (as iSPIRT notes).

Each option has trade-offs. For example, strong subsidies speed rural coverage but risk inefficient spending; strict regulations protect consumers but may slow private investment. Overall, solutions that enhance consumer benefit and inclusion (lower prices, more hotspots, easier use) score highly for NDCP-2018 compliance and long-term sustainability. Over-regulation or one-size-fits-all fixes could deter grassroots entrepreneurs; similarly, pure market-driven models falter in low-income areas without support. A balanced mix—combining market incentives with targeted support and user-friendly tech—appears most promising.

4. Recommendations (Key measures)

Based on the above evaluation, we recommend prioritizing the following measures:

- **Tariff parity and infrastructure sharing:** Ensure PDO backhaul is priced at no more than retail fiber rates[6] and enable shared use of BharatNet/FTTx infrastructure. This directly cuts PDO operating costs, making Wi-Fi affordable for consumers and viable for providers. It aligns with NDCP's aim of affordable broadband.

- **Seamless authentication and roaming:** Implement global Wi-Fi standards (Pass point/Hotspot 2.0) with UPI/Aadhaar eKYC, and adopt Open Roaming for cross-provider handover. This makes access frictionless for users, boosting uptake. For small PDOs, it simplifies technical setup (no captive-portal coding). A one-click experience can dramatically expand daily use (e.g. students using school Wi-Fi continuously).

- **Targeted financial support and revenue models:** Provide focused subsidies or viability-gap funding in low-demand regions. Simultaneously, enable new revenue streams: permit advertising, content bundling, and institutional tie-ups for PDOAs. These measures shore up PDOA/PDO revenue while keeping consumer prices low. They are consumer-centric (ensuring service reach and affordability) and bolster long-term industry health.

- **Awareness, training and ecosystem integration:** Launch an intensive PM-WANI publicity campaign through Gram Sabhas, schools, CSCs and media. Train local entrepreneurs (shopkeepers, tea-stall owners) in hotspot operations and kiosk models (as demonstrated successfully in Mirzapur[38]). Partner with CSC networks, tourism boards, railways and urban local bodies to host PDOs. This creates a robust demand-supply match and spreads digital literacy.

Policy Recommendation: *"We urge TRAI and DoT to enact a coordinated package of reforms: enforce broadband-parity tariffs and backhaul sharing, simplify user authentication (leveraging UPI/Aadhaar and global Wi-Fi standards), and launch targeted financial incentives for rural last-mile Wi-Fi. Coupled with a nationwide awareness drive and integration with CSCs, smart cities and public venues, these measures will expand affordable public broadband in line with NDCP-2018's inclusion goals. This balanced, consumer-centric approach will make PM-WANI truly sustainable and entrepreneur-friendly."*

5. Execution roadmap

Short term (0–1 year):

- **Regulatory actions:** DOT/TRAI should finalize the PM-WANI tariff order (capping PDO backhaul rates to twice retail fiber) and amend rules to remove OTP/KYC friction (enable Pass point/UPI login). Update PM-WANI guidelines to clarify licensing (explicitly no license needed) and streamline RoW permissions. Establish model RFPs for in-building Wi-Fi (NBC/MBBL inclusion).
- **Launch awareness campaign:** DoT and state governments to run "PM-WANI for All" drives via CSCs, panchayats, and social media. Highlight case studies (e.g. successful hotspots at tea stalls). Provide easily accessible registration kiosks at CSCs and train CSC operators as PDOA aggregators.
- **Initiate funding schemes:** Allocate Digital Bharat Nidhi/USOF grants for PM-WANI deployment, focusing on blocks with low coverage. Announce incentives (power-bill rebates, interest-free loans under SASCI[25]) for

PDOAs to use municipal fiber/ducts. Set up a VGF window for remote areas.

- **Pilot technology upgrades:** Encourage a few PDOAs to trial Pass point/APN integration with current apps; mandate that new PDOAs use Open WIFI-compliant APs. Coordinate with HFCL and others to supply affordable certified hardware. Test unified authentication/payment portals using UPI.

Medium term (1–3 years):

- **Scale network expansion:** States and ULBs adopt "Public Wi-Fi Plans" in smart city and Gram Panchayat budgets. Street furniture, bus terminals and government buildings are equipped with hotspots. District-level RoW committees (DM-led) are empaneled to expedite approvals.
- **Technology rollout:** Complete nationwide rollout of Pass point authentication and Open Roaming frameworks. PDOAs upgrade systems to support automatic user handover between hotspots. Develop a "super-aggregator" portal to coordinate roaming across all networks.
- **Capacity building:** Conduct ongoing training workshops for new PDO entrepreneurs. Encourage universities/technical institutes to develop PM-WANI toolkits. Integrate PM-WANI topics into entrepreneurship courses to sustain momentum.
- **Policy reviews and adjustment:** TRAI should establish quarterly monitoring of PM-WANI KPIs (hotspot count, user sessions, data consumed) via the Central Registry and public dashboards. Use these metrics to fine-tune policies (e.g. expanding subsidies if uptake lags). Schedule biennial reviews of PM-WANI rules with stakeholder feedback.

Roles of stakeholders:

- *Department of Telecom (DoT):* Lead policy reforms, disburse VGF/subsidy funds (Digital Bharat Nidhi, USOF), coordinate with States on BharatNet backhaul.
- *TRAI:* Finalize and enforce tariff orders, incorporate PM-WANI metrics into reports, mandate grievance redress channels for Wi-Fi (closing the current gap).
- *PDOAs/App Providers:* Adopt the technical upgrades (Open Roaming, Passpoint) and simplify user apps. Onboard new PDOs (especially local retailers) and manage voucher distribution.
- *ISPs/TSPs:* Abide by new pricing norms, offer wholesale plans to PDOAs, and promote public Wi-Fi as an offload layer (improving mobile QoS).
- *State Governments/ULBs:* Mobilize local infrastructure (fiber ducts, streetlights) and host institutions (schools, hospitals) as PDOs. Run awareness and digital literacy drives under state Digital India missions.
- *Civil Society/Industry Groups:* NGOs and BIF/Consumer Associations should help educate communities on using and running hotspots. Industry bodies can foster "public Wi-Fi incubators" for entrepreneurs.

Monitoring and review: TRAI and DoT should publish periodic performance reports (e.g. quarterly updates on hotspot growth and usage). Establish a cross-ministry PM-WANI task force to review progress and handle inter-agency issues. Ensure mechanisms for user complaints and remedy (e.g. integrate Wi-Fi service issues into the telecom grievance portal).

With these coordinated steps, PM-WANI can become a truly inclusive public broadband layer—earning consumer trust through affordable, reliable Wi-Fi, while rewarding the entrepreneurs who power it.

Q6. Are there improvements needed in the Authentication, Authorization, Roaming, and Payment architecture of the PM-WANI Framework? Please share suggestions, if any. Please provide your response in detail with justification.

Comments :

Executive Summary

PM-WANI's AARP (Authentication, Authorization, Roaming, Payment) module is central to user and PDOA/PDO experience. In practice it faces significant friction – users must register via an App and OTP, select packages, purchase vouchers, and log in at each hotspot – all of which deters usage. Meanwhile, no standardized roaming means users re-authenticate even within the same city. Payment by disposable vouchers is cumbersome, and limited revenues (many PDOs must charge modest fees) undermine commercial viability. Security and privacy concerns on open Wi-Fi cause users to default to mobile networks. These AARP shortcomings depress PDOA/PDO revenues (uncertain, low ARPU) and discourage new entrepreneurs (complex rules, low returns) while limiting consumer access, trust, and adoption.

To address these, we recommend:

(1) Adopting modern Wi-Fi standards (Pass point/Hotspot2.0, WPA3, EAP-based auth) and Open Roaming for seamless login and handover,

(2) Implementing a centralized, one-click payment/auth gateway (e.g. UPI-integrated login) to eliminate captive-portal vouchers,

(3) Standardizing revenue-share models and viability support for low-income areas, and

(4) Expanding awareness/training for small entrepreneurs. These measures (supported by international best practice and TRAI guidance) directly reduce consumer friction and improve trust, while ensuring entrepreneurial incentives and long-term sustainability.

Top 3–4 Recommendations: Mandate Pass point/Hotspot2.0 and Open Roaming adoption to enable instant, secure access; integrate PM-WANI apps with UPI (or similar) for one-click payment to eliminate voucher friction; define simple fixed revenue-share schemes (with viability gap funding in low-demand areas); and fund awareness/capacity-building for new PDOs. These reforms:

(a) align with NDCP-2018 goals of inclusive, affordable access,

(b) greatly enhance consumer experience and trust, and

(c) make small-shop Wi-Fi economically viable.

1. Define the Problem

Key AARP challenges: The current PM-WANI AARP design relies on a multi-step OTP/login process and isolated captive portals, causing user friction. Typical obstacles include:

Authentication/UX friction: Mandatory OTP logins, multiple apps/registrations, and one-time voucher purchases make “sign-on” slow and confusing for consumers. Especially for users with low digital literacy, these repeated steps are onerous compared to instant mobile-data access.

The DoT's 2009 OTP mandate persists in PM-WANI, even though modern secure methods exist. This complexity drives many users to avoid PM-WANI entirely.

Lack of seamless roaming: PM-WANI hotspots operate as isolated networks. Each new PDOA/PDO login requires re-authentication, yielding interrupted sessions when moving between access points. By contrast, cellular data "just works" across cells. Without standardized roaming protocols (e.g. IEEE 802.11u/Passpoint or OpenRoaming), handovers are clunky or impossible.

Payment complexity: Current model uses prepaid "vouchers" purchased via the App or website. This micropayment scheme is cumbersome – users must select and buy each small data pack through the app's portal. This friction (and fear of hidden costs) discourages sporadic users. Moreover, settlement across multiple wallets/cards requires coordination, raising administrative costs for PDOAs.

Commercial viability: Public Wi-Fi must compete with extremely cheap mobile data. India's average realized data price is only ~₹7.87/GB, so consumers expect free or near-free Wi-Fi. PDOs typically charge modest rates to cover backhaul costs, but low volume and competition from bundled telecom plans undermine revenue. Without clear, stable revenue shares (PDO gets X%, PDOA Y%), small entrepreneurs lack incentive to join. Capital costs (APs, backhaul equipment) and operating costs (electricity, ISP charges) further strain margins.

Security/privacy concerns: Unencrypted public Wi-Fi raises user fears. As TRAI notes, many users "prefer the perceived safety of mobile networks," and mistrust open hotspots for transactions. PDO operators (often small

shops) may lack expertise to deploy WPA3/EAP, leaving networks insecure. Any AARP workflow that logs phone numbers via OTP or exposes personal data also raises privacy and compliance issues.

Regulatory/compliance burden: Although PM-WANI is "licence-free," it still imposes registration and AML/KYC obligations on PDOAs and App Providers. Maintaining audit trails (per laws) adds to the burden. Small entrepreneurs may be deterred if compliance (billing, logging) is seen as complex or risky.

Impacts: These challenges hurt all stakeholders:

(a) PDO/PDOA Revenue Certainty & Sustainability: Low usage (due to UX and trust issues) leads to uncertain, sporadic revenue. Complex payment flow incurs administrative costs and attrition. The inability to roam limits each PDO's catchment to its immediate vicinity, capping growth. Cheap mobile data makes paid Wi-Fi unattractive, cutting into potential market. As a result, many PDOs struggle to cover even basic costs.

(b) Entrepreneur Participation: New or small entrepreneurs face steep onboarding: purchasing certified equipment, understanding technical setup, and navigating multi-party revenue splits (with App Providers, PDOAs, ISPs). The effort/reward ratio is poor when expected earnings are uncertain. Complex authentication rules (OTP, app stores, etc.) and opaque tariff models discourage non-technical small businesses.

(c) Consumer Access, Affordability & Trust: For users, current AARP design means unpredictable costs and slow login. Confusing payments (vouchers, different app UIs) undermine affordability and trust. Repeated logins reduce convenience, so coverage gaps remain: many Wi-Fi APs go

unused simply because users dislike the hassle. Additionally, privacy and security worries mean consumers often avoid Wi-Fi altogether, perceiving mobile data as safer. In sum, poor AARP UX throttles consumer adoption of PM-WANI, violating the NDCP goal of affordable ubiquitous broadband.

2. Explore Possible Solutions :

We propose a broad menu of interventions. Each targets specific challenges above:

Technical/Standards Enablers:

Pass point/Hotspot 2.0 and WPA3: Mandate WPA3 and 802.11u (Pass point) support for new PDO APs and user devices. Pass point enables automatic, secure authentication without captive portals, vastly simplifying logins. With Pass point, a user's device can store credentials and roam between networks without user action, addressing both login friction and roaming. This replaces the legacy OTP/captive-portal model and lifts a key bottleneck.

Federated Authentication (EAP-SIM/AKA): Leverage SIM-based EAP (or eKYC) so that mobile subscribers can authenticate using their SIM credentials or pre-verified identity, eliminating OTP. As in Singapore's Wireless@SG, EAP-SIM allows "auto-connect" to Wi-Fi. This improves security (SIM-chained credentials) and UX.

Open Roaming (WBA framework): Adopt the Wireless Broadband Alliance's Open Roaming federation for PM-WANI. Open Roaming uses standard Pass point credentials and a global federation of identity providers to allow seamless handover between providers. In practice, users authenticated to one PDOA could automatically connect at any other Open

Roaming-enabled hotspot. This “unifies” AARP by creating a common roaming pool, solving session continuity.

Super-Aggregator Architecture: Following TRAI’s suggestion, create (or designate) a “super aggregator” entity or central RADIUS/AAA hub that all PDOAs use for AAR duties. This centralizes tokens and settlement, ensuring any PM-WANI user credential is honoured nationwide. It simplifies authorization flows and inter-PDOA roaming.

Payment Innovations:

Unified Payment Gateway (UPI integration): Enable direct one-click top-ups via UPI/Wallet APIs. Instead of buying intermediate vouchers, the App can invoke UPI authorization (or BharatQR) for immediate micropayment. TRAI explicitly proposes a central auth/payment gateway via UPI to eliminate captive portals. This reduces steps to a single tap, greatly improving user convenience.

OAuth2/UMA for Payments: Consider using modern authorization frameworks (e.g. OAuth2/OpenID Connect) so that user devices can securely token-authorize payments or sessions with PDOAs without repeated identity input. For example, an OAuth flow between the App and PDOA could pre-authorize an account’s usage limits or payment credentials.

Tokenization/Wallet Credits: Issue digital Wi-Fi tokens or account credits (prepaid with cash or digital money) that work across PDOAs. A user could scan a QR code on a hotspot, add a small credit amount (via UPI or token), and consume it seamlessly—avoiding per-session checkouts. (This is akin to “offline mode” vouchers that are device-stored.)

Standardized Revenue-Sharing: Define clear default splits for revenue between PDO, PDOA, App Provider, and TSP. For example, a rule might allocate 50% of sale price to PDO, 30% to PDOA, 20% to App/TSP (or similar). Such standardization (possibly with caps or floors) reduces negotiation complexity and builds predictability for entrepreneurs. TRAI's tariff-order (2025) already capped ISP charges for PDOs, and a similar approach can fix margins among PM-WANI entities.

Policy and Regulatory Measures:

Mandate AARP Standards: Update PM-WANI regulations to require (or at least allow) Passpoint/EAP and OpenRoaming compliance. Remove the outdated 2009 OTP mandate, and formally permit Aadhaar-based eKYC or even allow users to log in via existing telecom credentials. This aligns with TRAI's 2016 vision of "one-click" auth.

Simplified Onboarding: Further relax compliance for small PDOs, such as streamlined KYC for micro-data packages or an initial "trial" usage limit before full ID collection. For example, allow anonymous or simplified login (just device ID) for first few sessions, then require full authentication.

Tariff & Incentive Frameworks: Build on the 2025 Tariff Order (capping FTTH rates for PDOs) by extending price ceiling / subsidized access to more cases. For instance, a special low-cost data plan for PM-WANI PDOAs could be mandated. Also, align PM-WANI with NDCP's Digital Bharat Nidhi fund or Smart City funds to subsidize AARP compliance costs in remote areas.

Encourage Public PPP Models: Officially permit and fund models where state/local bodies become PDOAs (as TRAI suggests). Government

agencies (Panchayats, CSCs, schools, hospitals) could aggregate local APs and share AARP infrastructure, reducing risk for each PDO.

Awareness and Capacity Building:

Education Campaigns: The government (DoT, TRAI, State IT departments) should run campaigns to inform consumers how to use PM-WANI (e.g. “Wi-Fi finder” apps, “join hotspots for one Rs per day!”), and entrepreneurs that becoming a PDO/PDOA is easy and license less.

Training & Support: Provide free tutorials or workshops (via CSCs or BSD networks) on setting up a PDO, using the App, pricing plans, and basic security. Possibly certify “PM-WANI enablement” for local ISPs/tech shops to help small merchants deploy compliant networks.

Integration with Other Schemes: Leverage existing public infrastructure: e.g. encourage all CSC kiosks or Ayushman centres to become PDOs (using BharatNet backhaul). Integrate PM-WANI app access points into tourist info, rail stations (as PM-WANI hotspots), urban transit systems, etc. For example, SSIDs at metro stations could carry the PM-WANI captive portal, while using centralized auth.

Technology & Infrastructure Enablers:

Cloud & Analytics: Promote a cloud-based PM-WANI management platform where PDOAs can monitor hotspots and usage. Use analytics to plan hotspot placement (like cell-site planning in telcos). Such tools reduce management overhead and enable data-driven expansion.

Open WIFI and Shared Backhaul: Encourage open-source solutions (e.g. TIP Open WIFI) for hotspot hardware to lower equipment costs. Foster backhaul sharing: municipal or telco fibre networks (BharatNet/Smart City)

could be shared by many PDOs to reduce per-PDO cost. Where fiber is absent, allow ISPs to use wireless backhaul (e.g. microwave or unlicensed 5GHz links) for PDOAs in rural areas.

Each solution above maps to specific problems. For instance, Passpoint/OpenRoaming tackle authentication and roaming issues; UPI-enabled one-click payments tackle **payment friction; revenue-share rules and subsidies bolster commercial viability; and awareness programs address low uptake and trust.

Trade-offs/Risks: Overhauling AARP has complexity. For example, Passpoint/OpenRoaming require upgrading equipment and standardizing across apps – this poses a risk of vendor lock-in or implementation delays, but yields maximal user benefit. Introducing a central payment gateway/UPI is relatively low-risk (leveraging India's mature UPI) but may raise concerns about data privacy and financial regulation if not designed carefully. Subsidies or grants can jump-start deployments in thin markets, but risk misuse and budgetary strain if not tightly monitored. Stricter KYC/eKYC improves trust but could exclude privacy-sensitive users. Mandating too many rules at once could overwhelm small PDOs. Hence, a balanced mix of low-hanging reforms (UPI, awareness) with phased technical upgrades is prudent.

4. Recommendation :

On balance, we prioritize measures that directly reduce user friction and empower small operators, while being cost-feasible. The top recommendations are:

1. Adopt Passpoint/Hotspot2.0 and WPA3: Mandate that new PDO equipment and apps support Passpoint authentication. Coupled with required WPA3 encryption, this eliminates manual logins and captive portals. Users would auto-connect to known networks, vastly improving UX and security. (Aligned with global best practice, this makes Wi-Fi "just work.")

2. Enable Seamless Roaming (OpenRoaming): Implement OpenRoaming or a national federated roaming scheme across all PDOAs. Practically, a user authenticated once can access any PM-WANI hotspot automatically. This removes major annoyance of re-authenticationand replicates the seamless cell coverage that consumers expect.

3. Streamline Payment/Auth with UPI: Require PM-WANI apps to integrate with UPI and other immediate-payment interfaces. This allows single-click purchase of data sessions and can combine login/payment in one step. By removing vouchers and OTP portals, users pay as easily as any e-commerce transaction.

4. Standardize Revenue Share & Support: Issue clear guidelines (via TRAI/DoT) on revenue splits so that PDOs and PDOAs know their minimum earnings. Complement this with targeted viability funding (e.g. DBN or Smart City grants) for regions where traffic is low. A stable economic model will attract entrepreneurs.

5. Awareness & Capacity Building: Launch nationwide awareness drives and hands-on training (through CSCs and local bodies) about PM-WANI's

benefits and simple registration. Educating consumers on finding and using hotspots, and training PDOs on secure setup, will build trust and usage.

These measures together address both consumer-centric and entrepreneurial needs. Passpoint/OpenRoaming and UPI significantly improve convenience and trust for users, likely boosting adoption. Standardizing finances and providing subsidies make the business case viable for local shops. All are in line with NDCP-2018's vision of inclusive, ubiquitous connectivity.

Policy Recommendation: TRAI should direct that PM-WANI's AARP be modernized through global Wi-Fi standards and centralized payment integration. Specifically, mandate Hotspot 2.0/Passpoint (and WPA3) authentication and Open Roaming federation for seamless login, and establish a unified UPI-based payment gateway. Additionally, fix clear revenue-share rules for PDOA/PDO and authorize targeted subsidies in low-income areas. This combination will remove user friction and revenue uncertainty, making public Wi-Fi more accessible, affordable, and sustainable.

5. Implementation Roadmap

A practical timeline with stakeholder roles is outlined below (see Figure 1). The roadmap balances quick wins (0–1 year) with deeper reforms (1–3 years), and embeds monitoring and review mechanisms.

Short-term (0–1 year):

DoT: Sgould Issue amended PM-WANI guidelines explicitly permitting Passpoint/802.1X/EAP methods and UPI integrations; simplify OTP/KYC

requirements (e.g. allow Aadhaar/UPI-based auth). Launch viability fund calls for grant proposals (via DBN/SASCI).

TRAI: Can Set interim tariff rules (e.g. mandate 60:40 rev-share split, cap ISP backhaul rates), and draft final standards for Pass point/Open Roaming. Host workshops for App Providers on UPI compliance.

PDOAs/App Providers: Begin updating systems: integrate UPI/Wallet APIs in captive portals; enroll in certification (C-DoT) for updated AARP protocols; enable QR code login where possible. Pilot Pass point login at select hotspots.

ISPs/TSPs: Should Ensure PM-WANI data plans meet affordability targets (e.g. offer high-GB plans at capped rates). Assist PDOs to share backhaul or use ISP mesh services.

State Governments/Local bodies: Should Identify state PDOAs (e.g. Panchayat-based). Promote PDOA formation via CSCs. Facilitate RoW and provide municipal assets/power concessions for hotspot installation.

Monitoring: TRAI/DoT to mandate data collection by PDOAs (uptime, sessions, revenue) via the Central Registry. Use dashboards to track adoption. Establish a PM-WANI grievance channel (could piggyback on existing DoT portal or a dedicated PM-WANI cell) for users and PDOs.

Medium-term (1–3 years):

Full Tech Rollout: Scale Pass point/Open Roaming nationwide. All new APs must be Hotspot2.0-capable. Expand “super-aggregator” federation so that any PM-WANI user can roam seamlessly across apps/PDOAs. Continuously upgrade apps and networks as device capabilities grow (Wi-Fi 6/7 readiness).

Sustained Awareness: Conduct iterative digital literacy camps focusing on Wi-Fi (e.g. as part of Jan Shikshan). Encourage local media to list hotspots (Google Maps integration). Provide "PM-WANI starter kits" for new PDOs.

Regulatory Review: TRAI to issue periodic consultation (e.g. annual) to adjust rules based on field feedback. Evaluate impact of subsidies and revise revenue-share as needed. Ensure alignment with NDCP goals.

Stakeholder Roles:

DoT: Oversee spectrum backhaul incentives (e.g. Wi-Fi in 6 GHz), coordinate DBN funds for rural Wi-Fi, and update Telecom Act/Wi-Fi rules if needed.

TRAI: Monitor compliance (are apps using Pass point? Are tariffs honoured?), enforce standards, and mediate disputes. Require PDOAs to submit periodic reports (user count, traffic, payments).

PDOAs: Onboard hotspots to new authentication regime. Educate their PDOs on revenue schemes. Report aggregated usage and settlement transactions to regulators.

App Providers: Integrate multi-standard auth (Passpoint, EAP) and UPI support. Provide user support for login issues. Participate in the roaming federation.

ISPs/TSPs: Promote PM-WANI as traffic offload. Offer backhaul (BharatNet, fiber) at preferential rates. Collaborate on bundling Wi-Fi add-ons for subscribers.

State/Local: Continue to act as PDOAs via Panchayats or Smart Cities. Use municipal Wi-Fi as backhaul when possible (e.g. streetlight fiber). Support community institutions to open Wi-Fi access (libraries, schools).

Consumers: Through user education (and app design), ensure clear consent for data use in PM-WANI apps (addressing privacy concerns). Provide feedback via the grievance platform.

Monitoring & Review: DoT/TRAI should establish metrics (e.g. number of authenticated sessions, average per-AP usage, dropout rates at login, complaint counts) and review quarterly. Set targets (e.g. 80% of hotspots using Pass point by Year 3). Implement a formal grievance redressal process (leveraging telecom consumer forums or TRAI's complaint portal) specifically for PM-WANI issues. Regularly measure consumer satisfaction through surveys. Finally, periodically revise PM-WANI rules (e.g. every 2 years) incorporating lessons from field data, new technology (e.g. 5G integration), and international developments.

International Example: Singapore's Wireless@SG program (IMDA) transitioned to Passpoint and SIM-based auth to make public Wi-Fi seamless for citizens. In Europe, WiFi4EU cities have deployed Open Roaming so that residents roam across networks with a single identity. Such best practices demonstrate the efficacy of our recommendations.

By following this roadmap, PM-WANI's AARP can evolve from a burdensome, fragmented system into a user-friendly, secure, and scalable public Wi-Fi platform – unleashing its promise for digital inclusion and entrepreneurship.

Q7. In the Indian context, which of the following models would be more appropriate for the proliferation of Public Wi-Fi?

a. b. A model where the Government actively ensures hotspot deployment through direct funding and implementation support,

including backhaul provision; or A model where the Government primarily ensures availability of robust backhaul infrastructure and intervenes in hotspot deployment only in cases of market failure. Please provide your response in detail with justification.

Comments :

Policy Choice and Context

India faces a strategic decision in expanding public Wi-Fi: should the Government directly fund and deploy hotspots (including backhaul), or should it focus on robust backhaul infrastructure and leave hotspot rollout to the market, stepping in only where market failures occur? This choice is critical for India's digital future. India's National Digital Communications Policy (2018) and National Broadband Mission aim for ubiquitous broadband and 10 Gbps campuses by 2025/30. The NDCP set an ambitious target of 10 million public Wi-Fi hotspots by 2022, yet today India has only ~0.4 million (PM-WANI data)– far below the ~8 million hotspots suggested by global benchmarks. This gap underlines the importance of the question: increasing hotspot coverage, especially in rural and underserved areas, is key to bridging the digital divide, enhancing e-education, e-health, and e-governance. The policy choice will shape affordability, inclusion and the pace of digital transformation for students, small businesses, gig workers and vulnerable communities.

2. Consumer Impact of Each Model

From the consumer perspective, the two models trade off access, affordability, and service quality:

Direct-Government Hotspots (Model A): Government-funded hotspots (often free or low-cost) can rapidly expand coverage, especially in unprofitable areas. As seen in Brazil's Wi-Fi Brasil program, over 15,000 hotspots (including ~10,000 in schools) have brought free high-speed Internet to vulnerable communities. Similarly, Indonesia's BAKTI public Wi-Fi has deployed thousands of village Wi-Fi hotspots in schools, health centres and community centres. For rural users, students, gig workers and MSMEs, such public Wi-Fi can mean affordable internet (often free or subsidized) at local hubs. This boosts affordability (users do not need expensive mobile data), improves access in remote areas, and promotes inclusion (e.g. schools with Wi-Fi enable remote learning, health clinics can send data online).

However, risks include inefficiency and delays. Large government projects may suffer bureaucracy and slow rollout. There is also the danger of

Market distortion: if free Wi-Fi is ubiquitous, private entrepreneurs (like neighborhood PDOs) may lack incentive to invest. Long-term sustainability is a concern – will government maintain and upgrade the networks? Fixed infrastructure might become obsolete without market competition. In some cases (as seen in early municipal Wi-Fi projects), low usage or technical glitches meant scarce benefit despite large expenditure. Thus, while Model A greatly improves access for marginalized groups, it risks public funds being spent on low-value deployments if not well-managed.

Backhaul-First / Market-Driven (Model B): Here, government invests in robust backbone (fiber, microwave, satellite) and ensures open access, while leaving hotspot deployment to private/commercial actors except where no one else will go. This approach generally leverages competition to

improve quality and user choice. Consumers benefit from potentially higher service quality and innovation: private Wi-Fi providers can tailor services (e.g. premium hotspots, value-added services) and might roll out Wi-Fi 6E/7 equipment faster. Affordability may be helped if multiple private or local PDOs compete on price. For urban areas and commercial centers (e.g. malls, tourist spots, transit hubs), the market model will likely cover demand efficiently.

However, the access risk is that private players may ignore low-ARPU regions. Rural villages, remote markets or low-income urban pockets might remain unserved if only left to market forces. The result could be persistent digital exclusion for students in far-flung hamlets, or gig economy workers without coverage. Additionally, without government-coordinated hotspot planning, deployment could be uneven – e.g. many hotspots in crowded cities but none in adjacent rural areas. Finally, relying on market for hotspots means some areas might get only mobile broadband (if at all) and lack Wi-Fi.

In summary, Model A strongly promotes inclusion and affordability for underserved groups but risks inefficiency and crowding out private initiative. Model B promotes efficiency and high-quality service through competition but risks leaving gaps where commercial viability is low. An ideal strategy must balance these, ensuring that no community is left offline.

3. Industry and Economic Implications

The choice of model also affects the telecom industry and investment climate:

Impact on PDOs, PDOAs, ISPs, Neutral Hosts: Under Model A, a large-scale government Wi-Fi rollout could effectively substitute for the nascent PM-WANI ecosystem of Public Data Offices (PDOs) and PDO Aggregators (PDOAs). If the government directly provides Wi-Fi, many local entrepreneurs (PDO operators) might lose revenue opportunities. Conversely, if government funds are used to bolster common infrastructure, neutral-host providers (like RailTel or CloudExtel) could flourish by sharing network assets. RailTel, for example, is a neutral-fiber provider with 61,000+ km of fiber and Wi-Fi in 6,100+ railway stations. Model B, by focusing on backhaul and open infrastructure, tends to catalyze neutral-host investment – it leaves "last-mile" Wi-Fi provisioning to private PDOs under the PM-WANI framework, potentially growing that market.

Private Investment Incentives: Direct government hotspot deployment (Model A) can crowd out private investment. Economic studies (e.g. on municipal internet provision) show public network projects often **crowd out more private fiber investment than they induce. In other words, heavy government entry into service markets can reduce private sector spending. In contrast, government investment in backhaul infrastructure (Model B) can crowd in private investment: by laying the fiber and towers, the government lowers the cost barrier for ISPs and PDOs. Service providers can focus on last-mile without risking huge CAPEX on backbone. Historical experience from India's BharatNet (USOF-funded fiber to villages) shows this effect: when first-mile connectivity is provided, operators are more willing to extend services to those areas.

Business Viability and Sustainability: Government-run Wi-Fi (Model A) must eventually be sustainable without subsidies. If every public hotspot is

free, revenue models for maintaining them become unclear. The Public Wi-Fi ecosystem in India (PM-WANI) was expressly designed as market-driven, with government as enabler. In Model A, government or PSUs would need ongoing funding for maintenance or to mandate private partners to run the networks (risking variable quality). In Model B, by ensuring backhaul availability and affordable transit (for example, requiring ISPs to sell fiber to PDOs at regulated rates as recently done), the private sector can find a sustainable business model for Wi-Fi.

Government Intervention – Crowd Out vs. Catalysis: Government intervention should be catalytic, not permanently crowding out the market. A permanent subsidy-driven Wi-Fi network could discourage entrepreneurs. On the other hand, well-designed interventions (e.g. one-time grants or PPP) can catalyze growth. For example, Pakistan and some Latin American countries have used “voucher” schemes (first-come-first-served subsidies) that spur many localized Wi-Fi projects without government owning them. The challenge is to avoid a situation where private players expect indefinite subsidies.

In sum, Model B (backhaul-first) generally preserves private-sector initiative and ensures sustainable business models, whereas Model A (direct hotspots) risks market distortion. However, targeted government support (for example, subsidies for private providers in unprofitable areas) can combine the benefits of both.

4. Technology and Future-Readiness

Any model must support India's 2030 digital goals and evolving technologies:

Fiberization and 5G/6G Densification: Future networks will be fiber-centric and 5G/6G-driven. India's National Broadband Mission 2.0 (NBM 2025–2030) emphasizes extending fiber to 270,000 villages and anchor institutions (schools, health centers) and leveraging 5G and satellite to ensure high-speed coverage. A backhaul-focused model aligns with this: building deep fiber and open access will also serve future 5G small cells and 6G networks. By contrast, a hotspot-first approach must still secure fiber backhaul for each hotspot; if government bypasses fiber and uses wireless backhaul alone, the solution won't scale for 5G densification.

Wi-Fi Evolution (6E/7) and Shared Infrastructure: Advances in Wi-Fi (Wi-Fi 6E/7) will offer gigabit speeds on unlicensed 6 GHz+ bands. For example, the FCC in the USA has opened 1.2 GHz of mid-band spectrum for Wi-Fi 6E. India will likely follow, enabling many more high-performance hotspots. Both policy models must accommodate this. A backhaul-first strategy naturally provides the capacity needed for dense 6E deployments. Hotspot-first must specify future-proof equipment and re-useable fiber links. Additionally, "neutral host" and shared backhaul architectures (e.g. shared trenches, poles, spectrum) will be key. For instance, operators like RailTel are already exploring shared RAN solutions at congested stations. Ensuring policies allow common ducts, open fiber access and unbundled backhaul will benefit either model but is more central to Model B.

Satellite and Non-Terrestrial Connectivity: By 2030, satellite broadband (LEO/NGSO constellations, high-throughput satellites) will complement ground networks, especially in remote areas. Government policy can

accelerate satellite backhaul use for hotspots. Indeed, Brazil's Wi-Fi program uses the SGDC-1 satellite to reach rural sites. India's space assets (e.g. GSAT satellites) or commercial LEO services can backhaul rural hotspots efficiently. A backhaul-first approach naturally includes satellite as just another backbone, whereas Model A must coordinate satellite links for each new hotspot – doable, but must plan for it.

Alignment with National Goals: India's digital infrastructure goals (universal gigabit connectivity, digital empowerment) demand a technology-neutral approach that maximizes uptime and capacity. Model B, with robust fiber and wireless infrastructure, supports upcoming demands (e.g. Smart Cities, IoT, Industry 4.0). Model A can also adopt new tech, but if it relies on older Wi-Fi or wireless standards, it risks becoming obsolete. Therefore, whichever model is chosen, policies must mandate periodic technology upgrades and mesh ability with evolving networks.

In summary, to be future-ready, the policy must prioritize scalable backhaul and flexible architectures (fiber, shared infrastructure, neutral-host models) while ensuring hotspots use the latest Wi-Fi and satellite tech. A backhaul-first orientation is more naturally aligned with India's 2030 vision, but targeted hotspot deployments should still employ Wi-Fi 6E/7 and leverage the expanded spectrum and fixed wireless access technologies.

5. International Best Practices

Global experience offers valuable lessons for India's context:

Government-Led Hotspot Deployment: Countries like Brazil, Indonesia and South Korea have used direct public funding to roll out thousands of hotspots in underserved areas. Brazil's Wi-Fi Brasil program (Ministry of

Communications + Telebras) has installed over 13,200 satellite-fed hotspots, serving 8.5 million people (80% in rural North/Northeast). It targets schools, health clinics, indigenous villages and community centers. Indonesia's BAKTI (Universal Service Obligation) similarly built **thousands of public Wi-Fi hotspots** in schools, clinics and villages. In South Korea, local governments provide free Wi-Fi in major public spaces and even national roaming plans. These models show that government deployment can dramatically improve rural and social inclusion.

Backhaul-First and Voucher Models: The European Union and Singapore have emphasized infrastructure and incentivized local rollout. The EU's WiFi4EU program provided €15,000 vouchers to ~3,400 municipalities (2018) to install public Wi-Fi. This "voucher" approach mobilizes local authorities without direct central deployment. Separately, the EU's Digital Decade goals focus on gigabit-capable networks (fiber/5G) before emphasizing public hotspots. Singapore (Wireless@SG) combined heavy investment in fiber/5G backhaul with free public Wi-Fi funded by the Infocomm Development Authority. Three operators deployed free island-wide Wi-Fi (target 512 kbps), covering most public venues. Singapore's model shows how government can set targets and coverage (model A), yet rely on operators (private PDOs) to implement them.

Hybrid/Contextual Approaches: Other nations blend strategies. For example, some US cities operate municipal Wi-Fi in public buildings (libraries, city centers) only where private service is lacking, and otherwise encourage private ISPs. The EU also encourages open access fiber (backhaul) through PPP, while funding hotspots via grants. In summary, no

major economy relies solely on direct federal hotspot rollout; instead, they combine infrastructure investment with targeted interventions.

Lessons for India: Government-led programs (Brazil, Indonesia) successfully reach schools and rural areas, but require strong project management and accountability. Voucher/PPP schemes (EU, Singapore) allow local choice and faster adoption with limited federal involvement. Crucially, these models often complement backbone buildout: e.g. WiFi4EU operates where fiber or broadband already exists. India should heed that market-based, neutral-host models (like Singapore's multi-operator approach) and data-driven site selection (based on traffic or deprivation indices) yield better outcomes than ad-hoc deployment.

6. Recommendation

A balanced hybrid model is recommended. India should **prioritize robust backhaul infrastructure nationwide, and **intervene in hotspot deployment only where market fails. Specifically:

Focus Government Efforts on Backhaul: The Government must continue to fund and accelerate fiberisation, shared wireless backhaul and satellite links (e.g. BharatNet, one-nation RoW rules, USOF towers). This ensures every village panchayat has a fiber point or tower, creating an open-access spine for all services. Affordable and non-discriminatory access to this backbone will catalyze private investment and new services.

Targeted Hotspot Deployment: Government should deploy or subsidize Wi-Fi hotspots only in low-viability areas – remote villages, marginalized urban pockets, government facilities (schools, health centers, panchayat

offices), and where socio-economic needs are greatest. These deployments should be clearly time-bound and catalytic (for example, a 3–5 year subsidy to prove viability) with sunset clauses. Once usage is established, operations can be transferred to PDOs/municipalities or sunset entirely. This avoids indefinite subsidies and encourages eventual self-sustainability.

Market-Driven Expansion Elsewhere: In commercially attractive zones (dense urban, highways, markets, transit hubs), leave hotspot rollout to private entrepreneurs under PM-WANI and local ISPs. The Government's role here is facilitative: ensure spectrum (e.g. 6 GHz for Wi-Fi 6E), mandate open access, and offer incentives (like Viability Gap Funding or tax breaks) if needed. This stimulates innovation and efficiency.

Justification: This hybrid approach combines the inclusion and affordability benefits of Model A (through targeted intervention) with the efficiency and innovation of Model B (through robust infrastructure and market competition). It aligns with India's digital decade: building backbone first (as envisioned by NBM) while not neglecting marginalized communities. The TRAI consultation itself notes that funding and intervention should vary by context (rural vs urban). Our recommendation follows this principle.

7. Governance, Accountability and Funding :

To implement the hybrid model effectively, a transparent, accountable framework and innovative funding are key:

Governance and Oversight:

Transparent Site Selection: Use data (mobile usage gaps, population density, socio-economic metrics) to identify where hotspots are needed.

Publish clear criteria. Engage local governments and communities in identifying public places (markets, schools, clinics) that require Wi-Fi.

Deployment Dashboards: Maintain a publicly accessible dashboard (akin to BharatNet progress) showing real-time hotspot rollouts, service levels and coverage maps. This ensures transparency and public scrutiny.

QoS Benchmarks: Establish minimum quality-of-service (QoS) standards for public Wi-Fi (e.g. minimum speeds, uptime, latency) and require operators (government or private) to meet them. Periodic speed tests and user feedback surveys can enforce these standards.

Third-Party Audits: Mandate independent technical audits of hotspot networks (as is done for telecom QoS) and public financial audits of subsidies. Include community participation (e.g. Gram Panchayat Digital Committees) to report issues at local level.

Data Protection and Accessibility: Ensure free/public Wi-Fi complies with privacy norms (no misuse of user data) and is accessible to people with disabilities (e.g. support for screen readers, signage).

Funding Mechanisms:

A mix of funding sources is needed. Possible mechanisms include:

Universal Service Obligation Fund (USOF): Leverage USOF for last-mile Wi-Fi in rural/tribal areas. USOF has funded BSNL's Village Wi-Fi and can be tapped for public hotspots in unserved areas.

Digital Bharat Nidhi (DBN): Utilize the new DBN infrastructure fund for broadband for connectivity projects, including last-mile Wi-Fi hotspots in deep rural areas. Where fibre runs up to a GP but no local Wi-Fi, DBN grants can fund the intervening links.

Viability Gap Funding (VGF): For PPP hotspot projects (e.g. high footfall corridors or smart city zones), provide VGF to make the business case. This was effective in road PPPs and can apply to digital infra (e.g. a bid process for setting up campus Wi-Fi).

PM-WANI/PMU-WANI Co-Funding: Encourage states and municipalities to co-finance hotspot projects (using 14th FC grants or CSR funds), since local bodies directly benefit. For example, states could top-up PM-WANI incentives for PDOs setting up hotspots in schools.

Public-Private Partnerships: Invite PPP models like jointly-built fiber and Wi-Fi projects (e.g. sharing costs between a private ISP and a state). The Government could provide existing assets (buildings, towers, poles) rent-free for hotspot APs under agreed commitments.

CSR and Philanthropy: Mandate or incentivize CSR contributions towards digital inclusion projects. Many Indian corporates could fund Wi-Fi at schools/clinics as part of CSR, especially in states where they operate.

Tax and Regulatory Incentives: Offer tax holidays or accelerated depreciation for broadband infrastructure (fiber deployment), and consider reduced license fees if providers meet public Wi-Fi targets.

These mechanisms should be deployed with clear eligibility criteria (e.g. only in underserved blocks), time limits, and performance conditions. For instance, a hotspot subsidy might require the operator to maintain 10 Mbps on average and cover 1,000 users per month, or else lose funding.

8. Phased Implementation Roadmap

A pragmatic multi-phase roadmap ensures orderly rollout and learning:

Phase 1 – Backhaul Strengthening: Prioritize fiber and tower upgrades in digitally backward districts. Complete BharatNet fiber to remaining 250k GPs and enable shared fiber usage (opening up excess capacity). Ramp up satellite broadband facilities (e.g. ground stations for LEO constellations) for remote zones. Ensure telecom towers have fiber backhaul or microwave links. Implement 6 GHz spectrum allocation for Wi-Fi 6E. By end of Phase 1, every district should have near-ubiquitous fiber/5G connectivity.

Phase 2 – Public Hotspot Deployment in Market-Failure Zones: Using the data-driven selection, launch government-supported hotspot projects in phase-1 areas where no private provider has set up Wi-Fi. This includes (a) Rural areas: schools, Panchayat offices, health centers, marketplaces, post offices, etc., in villages and small towns. (b) Urban poor enclaves: slum areas, labor colonies. (c) High Social Priority Sites: government-run schools, Anganwadis, public health centers, police stations, etc. Each project should have a finite concession period; after which it is expected that a local PDO or private entity will take over if viable.

Phase 3 – Market-Led Expansion with Incentives: In parallel, encourage private sector hotspot growth in commercially attractive areas. Incentivize operators and PDOs through tax benefits or small subsidies to install Wi-Fi in urban centers, tourist spots, markets and along highways. PM-WANI should continue to grow (now ~4.1 lakh hotspots); TRAI/tariff orders ensure PDOs get affordable backhaul (as recently mandated). Encourage neutral-host small-cell deployments (e.g. CloudExtel) to densify networks. Promote integration of existing private hotspots (cafes, offices, apartments) into the PM-WANI mesh (as now permitted) so more locations serve as public APs.

Phase 4 – Monitoring, Quality Enforcement and Consumer Protection: Continuously monitor deployment, enforce QoS and address consumer grievances. TRAI should collect and publish hotspot performance data, and have a quick redressal mechanism for users. Periodically audit the financials of funded projects for leakage. Adapt strategy based on outcomes (e.g. scale back direct funding if hotspots are thriving, or increase in stubborn dark zones).

Each phase should have clear milestones (e.g. number of new fiber kms, hotspots installed, users served) and periodic review (e.g. every 6–12 months) with stakeholder feedback (including civil society and consumer groups).

9. Conclusion – A Future-Ready, Consumer-Centric Strategy

India's digital future demands ubiquitous, affordable, high-quality connectivity for all citizens. The evidence and international experience suggest that a balanced, hybrid model is best: build a robust backhaul backbone now, and use targeted government intervention only where private deployment is unviable. This approach maximizes consumer benefits – rapid access and inclusion where it is needed most – while preserving the incentives and innovation of the market.

Affordability is served by subsidized or free Wi-Fi in unprofitable areas, but sustainability is ensured by engaging private players and using open-access infrastructure. The strategy is technology-neutral and forward-looking: it prepares India's networks for 5G/6G densification, fiberization, and next-generation Wi-Fi (Wi-Fi 6E/7) and satellite backhaul. Governance measures

(transparent site selection, dashboards, QoS standards, audits) and innovative funding (USOF, DBN, PPP, CSR) provide accountability and ensure value for public money.

In sum, we recommend that the Government commit to being a catalyst, not the sole provider of Public Wi-Fi: fund and build the backbone, then work as a facilitator for hotspot proliferation. This balanced policy – marrying Government support with private initiative – will create a sustainable, future-ready ecosystem that guarantees affordable connectivity for India's students, businesses, workers and communities. The result will be a resilient digital infrastructure that drives economic growth and inclusion through 2030 and beyond.

India faces a strategic decision in expanding public Wi-Fi: should the Government directly fund and deploy hotspots (including backhaul), or should it focus on robust backhaul infrastructure and leave hotspot rollout to the market, stepping in only where market failures occur? This choice is critical for India's digital future. India's National Digital Communications Policy (2018) and National Broadband Mission aim for ubiquitous broadband and 10 Gbps campuses by 2025/30. The NDCP set an ambitious target of 10 million public Wi-Fi hotspots by 2022, yet today India has only ~0.4 million (PM-WANI data)– far below the ~8 million hotspots suggested by global benchmarks. This gap underlines the importance of the question: increasing hotspot coverage, especially in rural and underserved areas, is key to bridging the digital divide, enhancing e-education, e-health, and e-governance. The policy choice will shape affordability, inclusion and the

pace of digital transformation for students, small businesses, gig workers and vulnerable communities.

2. Consumer Impact of Each Model

From the consumer perspective, the two models trade off access, affordability, and service quality:

Direct-Government Hotspots (Model A): Government-funded hotspots (often free or low-cost) can rapidly expand coverage, especially in unprofitable areas. As seen in Brazil's Wi-Fi Brasil program, over 15,000 hotspots (including ~10,000 in schools) have brought free high-speed Internet to vulnerable communities. Similarly, Indonesia's BAKTI public Wi-Fi has deployed thousands of village Wi-Fi hotspots in schools, health centres and community centres. For rural users, students, gig workers and MSMEs, such public Wi-Fi can mean affordable internet (often free or subsidized) at local hubs. This boosts affordability (users do not need expensive mobile data), improves access in remote areas, and promotes inclusion (e.g. schools with Wi-Fi enable remote learning, health clinics can send data online).

However, risks include inefficiency and delays. Large government projects may suffer bureaucracy and slow rollout. There is also the danger of

Market distortion: if free Wi-Fi is ubiquitous, private entrepreneurs (like neighborhood PDOs) may lack incentive to invest. Long-term sustainability is a concern – will government maintain and upgrade the networks? Fixed infrastructure might become obsolete without market competition. In some cases (as seen in early municipal Wi-Fi projects), low usage or technical glitches meant scarce benefit despite large expenditure. Thus, while Model

A greatly improves access for marginalized groups, it risks public funds being spent on low-value deployments if not well-managed.

Backhaul-First / Market-Driven (Model B): Here, government invests in robust backbone (fiber, microwave, satellite) and ensures open access, while leaving hotspot deployment to private/commercial actors except where no one else will go. This approach generally leverages competition to improve quality and user choice. Consumers benefit from potentially higher service quality and innovation: private Wi-Fi providers can tailor services (e.g. premium hotspots, value-added services) and might roll out Wi-Fi 6E/7 equipment faster. Affordability may be helped if multiple private or local PDOs compete on price. For urban areas and commercial centers (e.g. malls, tourist spots, transit hubs), the market model will likely cover demand efficiently.

However, the access risk is that private players may ignore low-ARPU regions. Rural villages, remote markets or low-income urban pockets might remain unserved if only left to market forces. The result could be persistent digital exclusion for students in far-flung hamlets, or gig economy workers without coverage. Additionally, without government-coordinated hotspot planning, deployment could be uneven – e.g. many hotspots in crowded cities but none in adjacent rural areas. Finally, relying on market for hotspots means some areas might get only mobile broadband (if at all) and lack Wi-Fi.

In summary, Model A strongly promotes inclusion and affordability for underserved groups but risks inefficiency and crowding out private initiative. Model B promotes efficiency and high-quality service through competition

but risks leaving gaps where commercial viability is low. An ideal strategy must balance these, ensuring that no community is left offline.

3. Industry and Economic Implications

The choice of model also affects the telecom industry and investment climate:

Impact on PDOs, PDOAs, ISPs, Neutral Hosts: Under Model A, a large-scale government Wi-Fi rollout could effectively substitute for the nascent PM-WANI ecosystem of Public Data Offices (PDOs) and PDO Aggregators (PDOAs). If the government directly provides Wi-Fi, many local entrepreneurs (PDO operators) might lose revenue opportunities. Conversely, if government funds are used to bolster common infrastructure, neutral-host providers (like RailTel or CloudExtel) could flourish by sharing network assets. RailTel, for example, is a neutral-fiber provider with 61,000+ km of fiber and Wi-Fi in 6,100+ railway stations. Model B, by focusing on backhaul and open infrastructure, tends to catalyze neutral-host investment – it leaves "last-mile" Wi-Fi provisioning to private PDOs under the PM-WANI framework, potentially growing that market.

Private Investment Incentives: Direct government hotspot deployment (Model A) can crowd out private investment. Economic studies (e.g. on municipal internet provision) show public network projects often **crowd out more private fiber investment than they induce. In other words, heavy government entry into service markets can reduce private sector spending. In contrast, government investment in backhaul infrastructure (Model B) can crowd in private investment: by laying the fiber and towers, the government lowers the cost barrier for ISPs and PDOs. Service providers can focus on last-mile without risking huge CAPEX on backbone. Historical experience

from India's BharatNet (USOF-funded fiber to villages) shows this effect: when first-mile connectivity is provided, operators are more willing to extend services to those areas.

Business Viability and Sustainability: Government-run Wi-Fi (Model A) must eventually be sustainable without subsidies. If every public hotspot is free, revenue models for maintaining them become unclear. The Public Wi-Fi ecosystem in India (PM-WANI) was expressly designed as market-driven, with government as enabler. In Model A, government or PSUs would need ongoing funding for maintenance or to mandate private partners to run the networks (risking variable quality). In Model B, by ensuring backhaul availability and affordable transit (for example, requiring ISPs to sell fiber to PDOs at regulated rates as recently done), the private sector can find a sustainable business model for Wi-Fi.

Government Intervention – Crowd Out vs. Catalysis: Government intervention should be catalytic, not permanently crowding out the market. A permanent subsidy-driven Wi-Fi network could discourage entrepreneurs. On the other hand, well-designed interventions (e.g. one-time grants or PPP) can catalyze growth. For example, Pakistan and some Latin American countries have used "voucher" schemes (first-come-first-served subsidies) that spur many localized Wi-Fi projects without government owning them. The challenge is to avoid a situation where private players expect indefinite subsidies.

In sum, Model B (backhaul-first) generally preserves private-sector initiative and ensures sustainable business models, whereas Model A (direct hotspots) risks market distortion. However, targeted government support

(for example, subsidies for private providers in unprofitable areas) can combine the benefits of both.

4. Technology and Future-Readiness

Any model must support India's 2030 digital goals and evolving technologies:

Fiberization and 5G/6G Densification: Future networks will be fiber-centric and 5G/6G-driven. India's National Broadband Mission 2.0 (NBM 2025–2030) emphasizes extending fiber to 270,000 villages and anchor institutions (schools, health centers) and leveraging 5G and satellite to ensure high-speed coverage. A backhaul-focused model aligns with this: building deep fiber and open access will also serve future 5G small cells and 6G networks. By contrast, a hotspot-first approach must still secure fiber backhaul for each hotspot; if government bypasses fiber and uses wireless backhaul alone, the solution won't scale for 5G densification.

Wi-Fi Evolution (6E/7) and Shared Infrastructure: Advances in Wi-Fi (Wi-Fi 6E/7) will offer gigabit speeds on unlicensed 6 GHz+ bands. For example, the FCC in the USA has opened 1.2 GHz of mid-band spectrum for Wi-Fi 6E. India will likely follow, enabling many more high-performance hotspots. Both policy models must accommodate this. A backhaul-first strategy naturally provides the capacity needed for dense 6E deployments. Hotspot-first must specify future-proof equipment and re-useable fiber links. Additionally, "neutral host" and shared backhaul architectures (e.g. shared trenches, poles, spectrum) will be key. For instance, operators like RailTel are already exploring shared RAN solutions at congested stations. Ensuring policies allow common ducts, open fiber access and unbundled backhaul will benefit either model but is more central to Model B.

Satellite and Non-Terrestrial Connectivity: By 2030, satellite broadband (LEO/NGSO constellations, high-throughput satellites) will complement ground networks, especially in remote areas. Government policy can accelerate satellite backhaul use for hotspots. Indeed, Brazil's Wi-Fi program uses the SGDC-1 satellite to reach rural sites. India's space assets (e.g. GSAT satellites) or commercial LEO services can backhaul rural hotspots efficiently. A backhaul-first approach naturally includes satellite as just another backbone, whereas Model A must coordinate satellite links for each new hotspot – doable, but must plan for it.

Alignment with National Goals: India's digital infrastructure goals (universal gigabit connectivity, digital empowerment) demand a technology-neutral approach that maximizes uptime and capacity. Model B, with robust fiber and wireless infrastructure, supports upcoming demands (e.g. Smart Cities, IoT, Industry 4.0). Model A can also adopt new tech, but if it relies on older Wi-Fi or wireless standards, it risks becoming obsolete. Therefore, whichever model is chosen, policies must mandate periodic technology upgrades and mesh ability with evolving networks.

In summary, to be future-ready, the policy must prioritize scalable backhaul and flexible architectures (fiber, shared infrastructure, neutral-host models) while ensuring hotspots use the latest Wi-Fi and satellite tech. A backhaul-first orientation is more naturally aligned with India's 2030 vision, but targeted hotspot deployments should still employ Wi-Fi 6E/7 and leverage the expanded spectrum and fixed wireless access technologies.

5. International Best Practices

Global experience offers valuable lessons for India's context:

Government-Led Hotspot Deployment: Countries like Brazil, Indonesia and South Korea have used direct public funding to roll out thousands of hotspots in underserved areas. Brazil's Wi-Fi Brasil program (Ministry of Communications + Telebras) has installed over 13,200 satellite-fed hotspots, serving 8.5 million people (80% in rural North/Northeast). It targets schools, health clinics, indigenous villages and community centers. Indonesia's BAKTI (Universal Service Obligation) similarly built **thousands of public Wi-Fi hotspots** in schools, clinics and villages. In South Korea, local governments provide free Wi-Fi in major public spaces and even national roaming plans. These models show that government deployment can dramatically improve rural and social inclusion.

Backhaul-First and Voucher Models: The European Union and Singapore have emphasized infrastructure and incentivized local rollout. The EU's WiFi4EU program provided €15,000 vouchers to ~3,400 municipalities (2018) to install public Wi-Fi. This "voucher" approach mobilizes local authorities without direct central deployment. Separately, the EU's Digital Decade goals focus on gigabit-capable networks (fiber/5G) before emphasizing public hotspots. Singapore (Wireless@SG) combined heavy investment in fiber/5G backhaul with free public Wi-Fi funded by the Infocomm Development Authority. Three operators deployed free island-wide Wi-Fi (target 512 kbps), covering most public venues. Singapore's model shows how government can set targets and coverage (model A), yet rely on operators (private PDOs) to implement them.

Hybrid/Contextual Approaches: Other nations blend strategies. For example, some US cities operate municipal Wi-Fi in public buildings (libraries, city centers) only where private service is lacking, and otherwise

encourage private ISPs. The EU also encourages open access fiber (backhaul) through PPP, while funding hotspots via grants. In summary, no major economy relies solely on direct federal hotspot rollout; instead, they combine infrastructure investment with targeted interventions.

Lessons for India: Government-led programs (Brazil, Indonesia) successfully reach schools and rural areas, but require strong project management and accountability. Voucher/PPP schemes (EU, Singapore) allow local choice and faster adoption with limited federal involvement. Crucially, these models often complement backbone buildout: e.g. WiFi4EU operates where fiber or broadband already exists. India should heed that market-based, neutral-host models (like Singapore's multi-operator approach) and data-driven site selection (based on traffic or deprivation indices) yield better outcomes than ad-hoc deployment.

6. Recommendation

A balanced hybrid model is recommended. India should **prioritize robust backhaul infrastructure nationwide, and **intervene in hotspot deployment only where market fails. Specifically:

Focus Government Efforts on Backhaul: The Government must continue to fund and accelerate fiberisation, shared wireless backhaul and satellite links (e.g. BharatNet, one-nation RoW rules, USOF towers). This ensures every village panchayat has a fiber point or tower, creating an open-access spine for all services. Affordable and non-discriminatory access to this backbone will catalyze private investment and new services.

Targeted Hotspot Deployment: Government should deploy or subsidize Wi-Fi hotspots only in low-viability areas – remote villages, marginalized

urban pockets, government facilities (schools, health centers, panchayat offices), and where socio-economic needs are greatest. These deployments should be clearly time-bound and catalytic (for example, a 3–5 year subsidy to prove viability) with sunset clauses. Once usage is established, operations can be transferred to PDOs/municipalities or sunset entirely. This avoids indefinite subsidies and encourages eventual self-sustainability.

Market-Driven Expansion Elsewhere: In commercially attractive zones (dense urban, highways, markets, transit hubs), leave hotspot rollout to private entrepreneurs under PM-WANI and local ISPs. The Government's role here is facilitative: ensure spectrum (e.g. 6 GHz for Wi-Fi 6E), mandate open access, and offer incentives (like Viability Gap Funding or tax breaks) if needed. This stimulates innovation and efficiency.

Justification: This hybrid approach combines the inclusion and affordability benefits of Model A (through targeted intervention) with the efficiency and innovation of Model B (through robust infrastructure and market competition). It aligns with India's digital decade: building backbone first (as envisioned by NBM) while not neglecting marginalized communities. The TRAI consultation itself notes that funding and intervention should vary by context (rural vs urban). Our recommendation follows this principle.

7. Governance, Accountability and Funding :

To implement the hybrid model effectively, a transparent, accountable framework and innovative funding are key:

Governance and Oversight:

Transparent Site Selection: Use data (mobile usage gaps, population density, socio-economic metrics) to identify where hotspots are needed. Publish clear criteria. Engage local governments and communities in identifying public places (markets, schools, clinics) that require Wi-Fi.

Deployment Dashboards: Maintain a publicly accessible dashboard (akin to BharatNet progress) showing real-time hotspot rollouts, service levels and coverage maps. This ensures transparency and public scrutiny.

QoS Benchmarks: Establish minimum quality-of-service (QoS) standards for public Wi-Fi (e.g. minimum speeds, uptime, latency) and require operators (government or private) to meet them. Periodic speed tests and user feedback surveys can enforce these standards.

Third-Party Audits: Mandate independent technical audits of hotspot networks (as is done for telecom QoS) and public financial audits of subsidies. Include community participation (e.g. Gram Panchayat Digital Committees) to report issues at local level.

Data Protection and Accessibility: Ensure free/public Wi-Fi complies with privacy norms (no misuse of user data) and is accessible to people with disabilities (e.g. support for screen readers, signage).

Funding Mechanisms:

A mix of funding sources is needed. Possible mechanisms include:

Universal Service Obligation Fund (USOF): Leverage USOF for last-mile Wi-Fi in rural/tribal areas. USOF has funded BSNL's Village Wi-Fi and can be tapped for public hotspots in unserved areas.

Digital Bharat Nidhi (DBN): Utilize the new DBN infrastructure fund for broadband for connectivity projects, including last-mile Wi-Fi hotspots in

deep rural areas. Where fibre runs up to a GP but no local Wi-Fi, DBN grants can fund the intervening links.

Viability Gap Funding (VGF): For PPP hotspot projects (e.g. high footfall corridors or smart city zones), provide VGF to make the business case. This was effective in road PPPs and can apply to digital infra (e.g. a bid process for setting up campus Wi-Fi).

PM-WANI/PMU-WANI Co-Funding: Encourage states and municipalities to co-finance hotspot projects (using 14th FC grants or CSR funds), since local bodies directly benefit. For example, states could top-up PM-WANI incentives for PDOs setting up hotspots in schools.

Public-Private Partnerships: Invite PPP models like jointly-built fiber and Wi-Fi projects (e.g. sharing costs between a private ISP and a state). The Government could provide existing assets (buildings, towers, poles) rent-free for hotspot APs under agreed commitments.

CSR and Philanthropy: Mandate or incentivize CSR contributions towards digital inclusion projects. Many Indian corporates could fund Wi-Fi at schools/clinics as part of CSR, especially in states where they operate.

Tax and Regulatory Incentives: Offer tax holidays or accelerated depreciation for broadband infrastructure (fiber deployment), and consider reduced license fees if providers meet public Wi-Fi targets.

These mechanisms should be deployed with clear eligibility criteria (e.g. only in underserved blocks), time limits, and performance conditions. For instance, a hotspot subsidy might require the operator to maintain 10 Mbps on average and cover 1,000 users per month, or else lose funding.

8. Phased Implementation Roadmap

A pragmatic multi-phase roadmap ensures orderly rollout and learning:

Phase 1 – Backhaul Strengthening: Prioritize fiber and tower upgrades in digitally backward districts. Complete BharatNet fiber to remaining 250k GPs and enable shared fiber usage (opening up excess capacity). Ramp up satellite broadband facilities (e.g. ground stations for LEO constellations) for remote zones. Ensure telecom towers have fiber backhaul or microwave links. Implement 6 GHz spectrum allocation for Wi-Fi 6E. By end of Phase 1, every district should have near-ubiquitous fiber/5G connectivity.

Phase 2 – Public Hotspot Deployment in Market-Failure Zones: Using the data-driven selection, launch government-supported hotspot projects in phase-1 areas where no private provider has set up Wi-Fi. This includes (a) Rural areas: schools, Panchayat offices, health centers, marketplaces, post offices, etc., in villages and small towns. (b) Urban poor enclaves: slum areas, labor colonies. (c) High Social Priority Sites: government-run schools, Anganwadis, public health centers, police stations, etc. Each project should have a finite concession period; after which it is expected that a local PDO or private entity will take over if viable.

Phase 3 – Market-Led Expansion with Incentives: In parallel, encourage private sector hotspot growth in commercially attractive areas. Incentivize operators and PDOs through tax benefits or small subsidies to install Wi-Fi in urban centers, tourist spots, markets and along highways. PM-WANI should continue to grow (now ~4.1 lakh hotspots); TRAI/tariff orders ensure PDOs get affordable backhaul (as recently mandated). Encourage neutral-host small-cell deployments (e.g. CloudExtel) to densify networks. Promote integration of existing private hotspots (cafes, offices, apartments) into the PM-WANI mesh (as now permitted) so more locations serve as public APs.

Phase 4 – Monitoring, Quality Enforcement and Consumer Protection: Continuously monitor deployment, enforce QoS and address consumer grievances. TRAI should collect and publish hotspot performance data, and have a quick redressal mechanism for users. Periodically audit the financials of funded projects for leakage. Adapt strategy based on outcomes (e.g. scale back direct funding if hotspots are thriving, or increase in stubborn dark zones).

Each phase should have clear milestones (e.g. number of new fiber kms, hotspots installed, users served) and periodic review (e.g. every 6–12 months) with stakeholder feedback (including civil society and consumer groups).

9. Conclusion – A Future-Ready, Consumer-Centric Strategy

India's digital future demands ubiquitous, affordable, high-quality connectivity for all citizens. The evidence and international experience suggest that a balanced, hybrid model is best: build a robust backhaul backbone now, and use targeted government intervention only where private deployment is unviable. This approach maximizes consumer benefits – rapid access and inclusion where it is needed most – while preserving the incentives and innovation of the market.

Affordability is served by subsidized or free Wi-Fi in unprofitable areas, but sustainability is ensured by engaging private players and using open-access infrastructure. The strategy is technology-neutral and forward-looking: it prepares India's networks for 5G/6G densification, fiberization, and next-generation Wi-Fi (Wi-Fi 6E/7) and satellite backhaul. Governance measures (transparent site selection, dashboards, QoS standards, audits) and

innovative funding (USOF, DBN, PPP, CSR) provide accountability and ensure value for public money.

In sum, we recommend that the Government commit to being a catalyst, not the sole provider of Public Wi-Fi: fund and build the backbone, then work as a facilitator for hotspot proliferation. This balanced policy – marrying Government support with private initiative – will create a sustainable, future-ready ecosystem that guarantees affordable connectivity for India's students, businesses, workers and communities. The result will be a resilient digital infrastructure that drives economic growth and inclusion through 2030 and beyond.

Q8. Is there a need to adopt separate strategies for Public Wi-Fi proliferation in rural and urban areas? If yes, suggestions may be provided. Please provide your response in detail with justification.

Comments :

Public Wi-Fi can bridge India's digital divide, but **rural and urban areas face distinct challenges and opportunities**. Urban areas already have broadband and high population density, demanding high-capacity, secure, and integrated networks (mesh architectures, indoor coverage). Rural areas often lack reliable power and fibre backhaul, have sparse populations and lower incomes, requiring **cost-effective, resilient deployments** (possibly solar-powered hotspots, satellite or microwave backhaul) and heavy subsidies or PPPs. This report concludes that **tailored strategies are needed**. Urban plans should leverage existing fibre, 6 GHz Wi-Fi (now de-licensed in India), and mesh networks to offload dense mobile data, with a mix of paid and free hotspots. Rural plans

should build on BharatNet fibre, use community or state-run models for coverage, include solar/battery power, and rely on subsidies (DBN/USOF, viability-gap funding) for viability. Common enablers include PM-WANI guidelines (PDO/PDOA architecture) and robust QoS/security standards (WPA3, 802.11u/Hotspot2.0 for roaming). We compare deployment options (Table 1), recommend a **phased rollout** (Pilots ➔ Scale-up) with clear responsibilities, and define KPIs (hotspots deployed, uptime, usage) and budgets. Estimated CAPEX per public hotspot (including AP, power, installation) may range from ₹50–150 thousand, varying by location and backhaul. Key risks (backhaul shortfall, vandalism, low uptake) can be mitigated via community engagement, alternative backhaul (e.g. satellite, LEO), and demand-generation programs (digital literacy). Official sources (TRAI, DoT/DBN, BharatNet) guide this plan.

1. Problem Definition and Context

Despite record subscriber growth, **India's broadband gap persists**, especially between cities and villages. Public Wi-Fi is seen as a **scalable access layer** complementary to 4G/5G: it can offload mobile traffic, provide low-cost bulk data, and extend fixed broadband benefits (FTTH speeds, low latency) without per-user wired connections. The government's policies (Digital India, NDCP 2018, BharatNet, PM-WANI, Smart Cities) aim for universal connectivity. Yet **deployment lags targets**: PM-WANI has ~333,300 hotspots by mid-2025, far below NDCP's 10 million target. This shortfall is more acute in rural/remote areas due to sparse population and infrastructure deficits. The central question: *Should rural and urban Wi-Fi strategies differ?* We analyze technical, economic, social, regulatory, and operational factors to answer this.

2. Urban vs Rural Differences

- **Population Density & Demand:** Urban zones have high user density and demand peaks (transport hubs, offices, malls); rural areas have sparse users with lower peak load. Urban networks must support many concurrent users (e.g. Delhi Metro, Bangalore campuses). Rural use may focus on villages/GPs with a few dozen users.

- **Existing Infrastructure:** Cities have dense fibre, towers, electricity; villages may only have BharatNet fibre at the Gram Panchayat, intermittent power, and less fibre beyond core. For example, BharatNet connects ~214,000 of 256,000 GPs, providing a fibre "backbone" into rural cores.

- **Mobility:** Urban deployments must handle moving users (metro Wi-Fi, city buses) requiring roaming (Hotspot 2.0). Rural users are mostly stationary.

- **Security & Vandalism:** Outdoor rural equipment is more exposed to weather and vandalism. Urban indoor hotspots are safer but suffer from congestion and interference.

- **Power Reliability:** Urban grids are mostly reliable; many rural areas face frequent outages. Rural Wi-Fi should include battery/solar backup and bulk-power solutions.

- **Affordability & Literacy:** Rural incomes and digital literacy tend to be lower. They rely more on free or subsidized services and need awareness campaigns. Urban users may pay for premium service or use ad-supported models.

- **Use Cases:** Rural usage often focuses on basic internet, e-governance, telemedicine, education; urban includes media streaming, smart city apps, enterprise Wi-Fi, IoT (smart lighting, traffic).

Implication: A “one-size-fits-all” plan is suboptimal. Solutions must be **adapted**: e.g., dense mesh APs vs. standalone village hotspots, solar power vs. grid, PPP vs. community ownership.

3. Technical Considerations

- **Access Technology:** Public Wi-Fi (IEEE 802.11 variants) is primary. Urban networks benefit from Wi-Fi 6/6E/7: high throughput, beamforming, multi-link (multi-band) support. Mesh deployments (multi-AP clusters) provide coverage in dense areas. Rural networks may use simpler fixed Wi-Fi APs.

- **Spectrum:** Wi-Fi uses unlicensed bands (2.4 GHz, 5 GHz, now lower 6 GHz is de-licensed in India). Rural areas could exploit TV white spaces (not yet in India) or newly de-licensed 6 GHz for long-range if allowed. Urban networks may lean on 5 GHz/6 GHz for capacity and offloading.

- **Backhaul:** Arguably the *linchpin*. Urban hotspots leverage plentiful fibre/microwave/5G backhaul with high capacity. Rural hotspots must rely on BharatNet fibre (to GPs), microwave links, satellite/LEO backhaul or 4G towers for last connectivity. For example, **mesh** Wi-Fi offloads congested urban mobile cells via fibre; in rural Gram Panchayats, one can install Wi-Fi hotspots fed by the BharatNet PoP. Backhaul spectrum (microwave/WiMAX) can bridge villages without fibre.

- **Equipment:** Urban APs are often indoor or industrial-grade outdoor, dense (dozens per campus). Rural APs need weather-proof casings, low-power

(solar-friendly) designs. Use of locally-supported, low-maintenance hardware is crucial.

- **Power:** Urban sites rely on grid (with backup UPS). Rural sites should include solar panels or batteries due to grid unreliability. Bulk power connections (aggregating multiple hotspots on one meter) and govt schemes (e.g. DBN allowance for solar) can help reduce OPEX.

- **Quality of Service (QoS):** In high-density zones, implement IEEE 802.11e/WMM for voice/video priority. Urban deployments might enforce minimum throughput/SLA (e.g., 2 Mbps/user) per regulatory guidelines.

- **Security:** Use WPA3/802.1X/EAP, secure authentication portals, and promote VPN/HTTPS for users. Public Wi-Fi must comply with IT Act for lawful interception and minimal data retention. Urban networks in smart cities may integrate AI-driven threat monitoring. Both rural and urban networks need user trust measures (captive portal disclaimers, no malware).

4. Economic and Business Models

- **CAPEX/OPEX:** Urban rollout benefits from economies of scale: one fibre or backhaul link may serve thousands of users. The CAPEX per user is lower when densification is possible. Rural hotspots, serving few users, have higher cost-per-user. We estimate a **per-hotspot CAPEX** (AP + installation + local backhaul) roughly ₹50k–₹150k; adding solar/storage can double costs. OPEX differences: site maintenance (rural sites cost more travel/servicing), power (if subsidized via solar, can reduce OPEX).

- **Funding & Subsidies:** Rural deployments often need subsidies or grants. The Digital Bharat Nidhi (USOF successor) funds 4G towers and rural broadband; similar support (DBN/USOF) may subsidize Wi-Fi in unprofitable areas. Urban deployments can be commercially funded (private ISPs, malls, transit agencies). Viability Gap Funding (VGF) or Universal Service Levy could support key rural hotspots (like schools, hospitals).

- **Revenue Models:** Several models exist:

- **Commercial:** Users pay via coupons (PDO collects fee). In Tier-1 cities, some hotspots (cafes, parks) may offer paid plans or ads.
- **Freemium/Public Service:** Government/ULBs sponsor free access (as in many municipal Wi-Fi projects). Advertisements or tourism/transport agencies sponsor networks.
- **PPP:** Shared costs between local govt and ISP. E.g., Gujarat's GISL (state ISP) uses PPP to light up public Wi-Fi.
- **Walled Garden Services:** Some propose only allowing access to gov portals (not recommended for inclusion).

- **Cost Recovery:** Urban models can recover costs from heavy data users, ads, or enterprise Wi-Fi-as-a-Service. Rural models may never break even without subsidy; focus is on social returns (education, agri info). Carbon credits or development funds (e.g. TTDF) could be tapped for green rural Wi-Fi.

- **Public-Private Partnerships:** Mixed models are often best. For example, **municipal PPP**: city provides infrastructure (power, sites), private partner installs and operates (like Mumbai's Aaple Sarkar Wi-Fi). State PPP:

Gujarat's GISL (government-PI JV) connects public spots using BharatNet. Community models (self-help groups or cooperatives) can work in villages with training and small incentives.

5. Social & Demand Considerations

- **Digital Literacy:** Lower in rural areas, so parallel awareness and training (Common Service Centers, Village Internet Kiosks) must be included. Urban citizens are more tech-savvy. Deployments should include user education (e.g. how to connect to WANI apps safely).

- **Use Cases:** Tailor services: Rural Wi-Fi hotspots might pre-load local e-Gov apps (land records, healthcare info, agri prices) and provide community telemedicine points. Urban hotspots could integrate with smart-city services (e-payments, public transport info, AR/VR tourism guides).

- **Affordability:** Flat-rate or low-cost hourly coupons. TRAI notes PM-WANI permits very low per-GB tariffs (₹0.99–6 per GB) – urban users can pay a bit more for convenience, rural users need near-free service (often subsidized). Special plans (e.g. free morning bandwidth for farmers).

- **Content Localisation:** Rural networks should host regional language portals and offline content caching (educational videos, health tutorials) to reduce backhaul load. Cities may emphasize English and global content.

- **Trust & Safety:** Privacy fears reduce usage. Ensure users give informed consent, limit data collection, and comply with privacy laws (GDPR-like where possible). Build trust by partnering with local leaders/CSRs.

6. Regulatory & Policy Framework

- **Licensing:** Public Wi-Fi via PM-WANI is licensed light – PDOs register with DoT but require no spectrum licence. All PDOA/PDO participation lowers entry barriers. Rural strategy must ensure these entities (even local shops) can become PDOs easily. There is no separate “urban wifi licence” – it's all under WANI.

- **Spectrum Policy:** India has de-licensed lower 6 GHz band, boosting capacity. Policies should encourage equipment certification (Wi-Fi Alliance, WPC). The government might allocate mid-band (like 6 GHz) to unlicensed to ease congestion in cities.

- **Security & Privacy Standards:** TRAI calls for compliance with WPA3, secure portals, and minimal data collection. Urban networks must meet strict QoS (e.g. limiting latency for AR/VR). Regulations should allow lawful interception for crime prevention.

- **Right-of-Way (RoW):** As TRAI notes, simplifying RoW is critical (pole mounting, municipal assets). States should adopt unified RoW rules to speed installation of hotspots/poles in rural and urban areas.

- **Quality of Service:** Though no formal QoS norms yet for public Wi-Fi, operators are encouraged to follow IEEE 802.11e/WMM and ensure stable throughput. Regulators may set minimal throughput standards (e.g. 10-20 Mbps per hotspot, or 2 Mbps per user) especially for funded deployments.

- **Interoperability & Roaming:** Current Wi-Fi in India is fragmented (each PDOA or ISP is siloed). Mandating Passpoint (Hotspot 2.0) or an equivalent roaming exchange would help users move between networks seamlessly.

- **Funding & Incentives:** Policies like Digital Bharat Nidhi (DBN) provide funds for rural networks; extending similar schemes (DBN extension) to include Wi-Fi hotspots (beyond towers) is advisable. USOF/DBN may offer CAPEX subsidies for Wi-Fi in uneconomic areas.

- **Safety Regulations:** Equipment must meet standards (IP-rating, surge protection). Mandatory signage of official hotspots, user data protections (per IT Rules).

7. Operational & Implementation Considerations

- **Site Selection:**
- *Urban:* High-footfall, congested indoor/outdoor public spaces (metro stations, bus stands, markets, tourist spots, campuses).
- *Rural:* Key village locations (Panchayat office, health center, schools, markets).

- **Maintenance:**

- Urban networks can use professional crews and contracted maintenance.
- Rural networks benefit from “digital sahayaks” (local tech operators trained to maintain), reducing downtime. Parts distribution centers in district HQs can expedite repairs.

- **Local Capacity Building:** Train locals as PDOs or operators. E.g., in Gram Panchayats, ASHA workers or school teachers can oversee Wi-Fi points. Partner with NGO/CITC (like IIT initiatives) for rural digital literacy.

- **Vandalism/Theft Mitigation:**

- Use tamper-proof enclosures, GPS tracking, community ownership (social pressure).

- Involve Panchayats/police for security.
- Bulk billing and locking boxes together (e.g. sharing power lines) as recommended.

- **Performance Monitoring:** Install network management systems for real-time monitoring (uptime, usage). TRAI and local bodies should publish hotspot status dashboards (like BharatNet live).

- **Data Analytics:** Use usage data (anonymized) to optimize placement. For example, tracking peak usage at rural hotspots can indicate where more hotspots are needed (in schools during evenings, etc.).

- **Awareness & Demand Generation:** Conduct village panchayat meetings and urban street campaigns to promote the service. Leverage Digital India trainers to show benefits.

8. Options and Comparative Assessment

Strategy/Model	Description	Rural Viability	Urban Viability	Key Trade-offs
PM-WANI (Commercial PDOs)	Purely private rollout: any shop/individual can register as PDO, deploy paid/free hotspot with internet bought from ISP.	May not spontaneously serve remote villages (low ROI). Requires motivated PDOs in villages; many remain unserved.	Feasible in dense areas with paying customers (cafés, libraries, stations).	**+** Low govt burden; flexible. **–** Fragmented coverage; rural areas often skipped; limited traffic aggregation.
State/UT-led Wi-Fi (PPP)	State government designs network, uses PSU or local ISP (e.g. GISL Gujarat) and BharatNet for backbone.	High: e.g. a GP-level free Wi-Fi using BharatNet; can subsidize via state budget or donor. Depends on state capacity.	Moderate: cities can have state-run free hotspots (like Telangana Hy-Fi). Urban extensions easier	**+** Better coordination (single operator); can target unprofitable areas; unified branding. **–** Requires strong

Strategy/Model	Description	Rural Viability	Urban Viability	Key Trade-offs
			due to existing infra.	state capacity; risk of slow rollout or bureaucratic delays.
Municipal Wi-Fi (Smart Cities)	City/local body provides hotspots in key areas (metro, parks, gov offices) often via smart city budgets or PPP.	Low in villages (no municipal structure).	High in major cities; integrated with city services. Eg. Delhi/Mumbai.	**+** Integrated planning; leverages civic facilities (streetlights, poles). **–** Limited coverage to city limits; duplication if not aligned with state/PM-WANI.
Community Networks / NGOs	Local cooperatives or NGOs run mesh networks for villages; may use UHF/TVWS or Wi-Fi.	Medium: Engages villagers; examples in other countries (Nepal, etc.). Requires training.	N/A (primarily for underserved rural pockets).	**+** Empowers communities; may use innovative tech. **–** Sustainability issues; often requires external support.
Hybrid (PPP + Subsidy)	Private operator builds networks in return for subsidies or revenue-sharing (e.g. VGF, grants).	High potential: reduces operator risk in unprofitable rural projects.	Encourages wider deployment (operators get ROI via subsidies).	**+** Leverages private efficiency; ensures rollout in tough areas. **–** Needs good contract design and fund availability.

Table 1: Comparison of Public Wi-Fi deployment models for rural vs urban India.

Each model has pros/cons. In practice, a **blended approach** is best: combine PM-WANI private rollout in market-friendly zones, state/municipal projects in targeted areas, and PPP incentives for the rest. For example, BharatNet-linked GP hotspots (state model) can cover villages, while operators use PM-WANI to densify cities.

9. Recommendation & Phased Rollout Plan

Recommended Strategy: Adopt *differentiated approaches* with unified oversight. Specifically:

- **Urban Areas:** Focus on **mesh-based, high-capacity hotspots** in smart-city projects, transit hubs, campuses. Leverage private sector (PM-WANI) in commercial zones (malls, cafes), while government subsidizes core backhaul (e.g. new fibre to transit points). Enable city bodies to add free Wi-Fi in public spaces via PPP (as in Bangalore's Hy-Fi[30]). Use licenced 6 GHz and encourage Passpoint for seamless roaming.
- **Rural Areas:** Center on **BharatNet-based Wi-Fi**. Every connected Gram Panchayat or group of villages should host at least one free hotspot (via PDO/GP office or CSO), using state or centrally-funded PPP. Provide solar power and local technical support. Encourage Sanchalak (Village Wi-Fi entrepreneurs under BharatNet guidelines) to manage Wi-Fi. Supplement with satellite (LEO) links in very remote regions. Strongly subsidize CAPEX/OPEX through DBN and state funds, and consider viability gap funding for backbone.

Milestones and Responsibilities:

- *Phase 1:* DoT/TRA I define minimum standards (bandwidth, security, WANI compliance), DBN opens funding calls. Pilots: e.g. 10 urban hotspots

(Delhi Metro, IIT campus) and 20 rural GP hotspots. KPIs: pilot uptime ≥95%, usage data.

- *Phase 2:* Scale urban (metros, smart cities) and rural (select 20% of BharatNet GPs in each state). Appoint State DBN nodal officers, engage local NGOs for rural skilling. Deploy 1M+ hotspots nationally (e.g. 200K urban, 800K rural sites). KPIs: Hotspots deployed, % uptime, user sessions.
- *Phase 3:* Complete nationwide coverage, optimize based on analytics, integrate with 5G slices and IoT (Wi-Fi offload hotspots in 5G networks). KPIs: 2.5M hotspots by end-2030, 90% populated covered, data usage targets.

Budget Ranges: (Indicative) For initial estimate (assuming no fixed budget given):

- Urban hotspot (including backhaul lease): ₹50–100k CAPEX; ₹5–15k/yr OPEX.
- Rural hotspot (including solar, enclosure): ₹100–150k CAPEX; ₹10–20k/yr OPEX.

  Aggregated: If targeting 500K rural sites and 200K urban sites, CAPEX ≈ ₹70–80 billion (across 4-5 years), plus similar OPEX per year. Subsidies would cover much of rural CAPEX. These numbers are illustrative; detailed financial modeling should refine them.

Key Performance Indicators (KPIs)

- **Coverage:** % of population in target areas within 50 m of a hotspot (Rural vs Urban targets).
- **Hotspots Deployed:** Number of active public Wi-Fi APs (disaggregated Rural/Urban).

- **Utilization:** Monthly user sessions and GB of data used on public Wi-Fi.
- **Quality:** Uptime ≥98%, average throughput per AP (e.g. ≥50 Mbps).
- **Adoption:** Digital literacy workshops conducted, increase in rural internet penetration (per Rajya Sabha data).
- **Sustainability:** Reduction in cost per GB (e.g. target Wi-Fi ≤ ₹0.50/GB)[9], % of sites on renewable power.

Here, **DoT/DBN** provides funding (via USOF/DBN) and policy; **TRAI/BIS** sets standards (security, QoS); **State Governments/ULBs** coordinate local rollout, PPP agreements and local regulations; **TSPs/ISPs or aggregators** build and operate hotspots; **Local bodies** facilitate sites and power; **Citizens** are the end users, with feedback loops via usage data. Community groups (not shown) can also operate hotspots in rural areas under PDO model.

10. Risk Analysis and Mitigation

- **Low Adoption (especially rural):** Risk that citizens don't use Wi-Fi due to low awareness or preference for mobile data. *Mitigation:* Intensive awareness/digital literacy campaigns; incentivize initial use (e.g. first 1 GB free); bundle Wi-Fi into public services (e.g. eGov kiosks).
- **Vandalism/Power Theft:** Infrastructure damage or illegal tapping. *Mitigation:* Hardened enclosures, community ownership (Panchayat "adopts" hotspot), remote monitoring alarms, and governmental penalties.
- **Backhaul Shortages:** If BharatNet rollout delays or lacks capacity, hotspots stall. *Mitigation:* Use alternative backhaul (satellite/LEO services – e.g. Starlink, OneWeb); wireless microwave; interim 4G fallback. Allocate dedicated fiber for Wi-Fi at BharatNet GPs via MoU with DoT/BBNL.

- **Funding Delays:** Bureaucracy could slow subsidy disbursement. *Mitigation:* Set clear budget lines; private co-funding; use DBN's digital portals for transparency.
- **Cybersecurity Attacks:** Open networks could be abused for crime. *Mitigation:* Strict logging, real-time threat detection (TRAI notes AI-based security system for smart cities), user authentication controls.

11. Case Studies and Precedents

- **Kerala (Urban & Rural):** The K-Fi project offers free Wi-Fi at 2000+ points. It integrates with KFON fiber to reach BPL homes. Shows state PPP can combine rural fibre with public hotspots.
- **Telangana "Hy-Fi" (Urban):** ~3000 hotpots across Hyderabad (metros, schools, hospitals) under digital Telangana. Demonstrates city-level focus and dual use (mobility and fixed).
- **BharatNet (Rural Backbone):** Over 214,000 GPs fiber-connected. As of Dec 2024, Phase I/II enabled ~104k Wi-Fi hotspots (1–5 per GP)[32], boosting rural broadband subscribers from 115m to 405m (FY16–FY25). This huge infrastructure paves the way for Wi-Fi in villages.
- **International – South Korea:** Government-built dense Wi-Fi (94k hotspots) feeding from ubiquitous fibre; part of an integrated digital infrastructure. Their success attributes: aggressive government push, free access, citywide coverage. Suggests India's urban strategy should emulate coordinated fiber+Wi-Fi build.
- **EU WiFi4EU:** 93k municipal hotspots funded by the EU, showing local bodies deploying hotspots can achieve scale with minimal subsidy (5000€ voucher each). Indian cities could adopt similar "smart Wi-Fi zone" vouchers.

- **Africa/Asia Models:** (World Bank PPP case) Often, shared infrastructure (towers, fiber) lowers costs. Community networks (e.g. Nepal's village networks) succeed where local engagement is strong, highlighting social model viability.

These examples reinforce that **context matters**: free and dense in cities (to decongest), shared and subsidized in villages (to be affordable).

12. Conclusion

A differentiated strategy is **essential** for effective public Wi-Fi proliferation in India. The urban approach must emphasize capacity, integration and commercial viability; the rural approach must emphasize affordability, subsidy and resilience. By leveraging existing initiatives (BharatNet, PM-WANI), introducing supportive policies (simplified RoW, subsidies, spectrum liberalization), and engaging all stakeholders from panchayats to startups, India can accelerate digital inclusion. The plan above outlines a comprehensive path: from policy to pilots, through scale-up, underpinned by metrics and case-backed justification. With vigilant implementation and monitoring, both rural and urban populations can gain reliable, affordable public Wi-Fi, fulfilling national broadband and development goals.

Q9. What measures can be taken to improve the deployment and uptake of Public Wi-Fi networks in high-footfall areas for both outdoor (such as bus stops, roadside transit points, open public parks, markets, tourist sites), and indoor (such as airports, railway stations, malls, public institutions)? Please provide your response in detail with justification,

separately for outdoor and indoor scenarios. B. Role of Government-Funding deployments

Comments :

Public Wi-Fi has emerged as an essential component of India's digital public infrastructure, particularly in high-footfall areas where mobile networks often experience congestion and users require reliable, affordable, and easily accessible broadband connectivity. High-footfall environments, however, differ significantly in their operational characteristics. Outdoor locations such as bus stops, transit points, parks, markets, and tourist sites face challenges related to power, backhaul, and environmental exposure, whereas indoor locations such as airports, railway stations, malls, and public institutions demand high-capacity, carrier-grade Wi-Fi with seamless user experience. Therefore, a differentiated and context-specific approach is necessary to improve both deployment and uptake.

2. Measures for Outdoor Public Wi-Fi Deployment and Uptake

Outdoor high-footfall areas present unique constraints that directly affect the viability and performance of public Wi-Fi networks. These include low commercial returns for operators, unreliable power supply, limited backhaul availability, exposure to weather and vandalism, and low user trust due to security concerns. To address these issues, a set of coordinated measures is required.

The first measure is the integration of Wi-Fi access points with existing street infrastructure. Municipal assets such as smart poles, bus shelters, metro pillars, CCTV poles, and public buildings should be utilised for mounting outdoor Wi-Fi equipment. This approach significantly reduces capital

expenditure, avoids duplication of infrastructure, and accelerates deployment timelines.

The second measure is the adoption of mesh-based outdoor Wi-Fi architecture. Mesh networks provide resilient and scalable coverage in open areas where fibre connectivity may not be consistently available. They also allow for flexible expansion as footfall increases.

The third measure involves the use of hybrid backhaul solutions. Fibre should be used wherever feasible, but in locations where fibre is unavailable or unreliable, wireless backhaul options such as microwave, millimetre-wave, or even 4G/5G-based backhaul can be deployed. Solar-powered kiosks may be used in areas with unstable grid power.

The fourth measure is the adoption of sustainable business models. Outdoor Wi-Fi can be supported through advertising-based models, sponsorships, or freemium structures where basic data is provided free of cost and higher-speed or extended-duration plans are offered at nominal charges. Such models improve the financial viability of Public Data Offices (PDOs).

The fifth measure is the implementation of seamless roaming and a common SSID across public Wi-Fi networks. Technologies such as Hotspot 2.0 and Passpoint enable automatic authentication and eliminate repeated login friction, thereby improving user adoption.

The sixth measure is the development of a national Public Wi-Fi locator application. A simple interface that displays nearby hotspots, signal strength, and availability will significantly increase utilisation.

Finally, user trust must be strengthened through visible security certification. A “TRAI Certified Secure Wi-Fi” tag, combined with WPA3-based encryption, will reassure users and encourage wider adoption.

3. Measures for Indoor Public Wi-Fi Deployment and Uptake

Indoor high-footfall environments such as airports, railway stations, malls, and public institutions require a different set of interventions due to their controlled physical layout, high user density, and demand for consistent high-quality connectivity.

The first measure is the deployment of centralised Wi-Fi management platforms. A unified controller enables real-time monitoring, performance optimisation, and enhanced security across large indoor venues.

The second measure is the adoption of seamless authentication mechanisms such as Hotspot 2.0 and Passpoint. These technologies eliminate repeated login requirements and significantly improve user experience, especially in locations where users spend longer durations.

The third measure is the enforcement of QoS-based bandwidth allocation. Indoor venues often experience peak-hour congestion, and therefore, bandwidth must be dynamically managed to ensure stable performance for video streaming, conferencing, and other high-demand applications.

The fourth measure is the adoption of the neutral-host Wi-Fi model. This allows multiple telecom operators to share the same Wi-Fi infrastructure, reducing duplication, improving quality, and ensuring uniform user experience across networks.

The fifth measure is the integration of Wi-Fi authentication with India's Digital Public Infrastructure. Optional login through UPI, Aadhaar, DigiLocker, or venue-specific applications simplifies access and enhances convenience.

The sixth measure is the implementation of strict service-level agreements. Indoor public Wi-Fi must meet carrier-grade standards for uptime, latency, and repair timelines to ensure reliability in high-density environments.

4. Role of Government in Funding Deployments

Government intervention is essential to ensure widespread and equitable deployment of public Wi-Fi, particularly in outdoor and semi-commercial locations where private investment alone may not be viable.

The first role of Government is to provide Viability Gap Funding. A support mechanism covering 30 to 50 percent of capital expenditure for outdoor and low-revenue hotspots will significantly improve the financial feasibility of deployments.

The second role is to promote Public-Private Partnerships. A coordinated model involving Central Government, State Governments, Municipal Bodies, and private operators ensures shared risk, efficient deployment, and sustainable operations.

The third role is to monetise municipal assets. Local bodies should provide sites, power connections, and right-of-way permissions at concessional rates to reduce deployment barriers.

The fourth role is to utilise the Universal Service Obligation Fund for targeted support. High-footfall but low-income areas such as bus stands in small towns or public markets can be prioritised for subsidised Wi-Fi deployment.

The fifth role is to introduce voucher-based support for municipalities. Fixed-value vouchers for hotspot installation, similar to international models, can accelerate deployment in public spaces.

Finally, Government must establish a performance-linked disbursement framework. Funding should be tied to measurable indicators such as uptime, usage, and quality of service. A national dashboard should be created to monitor hotspot performance, ensure transparency, and enable data-driven policy refinement.

5. Conclusion

Improving the deployment and uptake of public Wi-Fi in high-footfall outdoor and indoor areas requires a combination of infrastructure integration, seamless authentication, strong quality-of-service standards, and sustainable business models. Government support through Viability Gap Funding, Public-Private Partnerships, municipal participation, and performance-based monitoring is essential to ensure scale, reliability, and long-term sustainability. With these measures, India can build a robust, secure, and user-friendly public Wi-Fi ecosystem that advances national digital inclusion goals.

A. OUTDOOR PUBLIC WI-FI (High-Footfall Open Areas)

(Bus stops, parks, markets, tourist sites, transit corridors)

Structured Policy Evaluation Table

Component	Detailed Analysis	Justification (Regulatory + Ground Reality)
Problem Definition	• Low commercial viability of PDOs in open areas • Lack of reliable power & backhaul • High vandalism & maintenance issues • Low user trust (security concerns) • Poor discoverability of hotspots	TRAI notes under-utilisation, low PDO viability, and trust deficit as key bottlenecks
Possible Solutions	1. **Street Infrastructure Integration** (smart poles, bus shelters) 2. **Mesh-based Wi-Fi architecture** 3. **Ad-supported + Freemium models** 4. **Common SSID + roaming (Hotspot 2.0)** 5. **Public Wi-Fi locator app (national)** 6. **Security certification (WPA3, trusted network tag)**	Aligns with global models (e.g., Seoul smart city mesh deployments) and TRAI emphasis on scalable architectures
Evaluation of Options	• **Infrastructure integration** → High ROI, reduces capex duplication • **Mesh networks** → Best for outdoor resilience & scalability • **Ad model** → Viable but limited in low-income areas • **Roaming/SSIDs** → Critical for seamless experience • **Apps** → Improves utilisation significantly • **Security certification** → Directly addresses trust deficit	Mesh + infrastructure reuse aligns with dense urban requirements highlighted in paper (high-density, multi-user environments)
Judgement (Best Strategy)	**Integrated Smart Infrastructure + Mesh Wi-Fi + Federated Access Model** is the most viable approach	Combines cost-efficiency, scalability, and user adoption simultaneously
Execution Framework	**Phase 1: Infrastructure Mapping** • Identify poles, bus stops, municipal assets **Phase 2: Deployment Model** • PPP-based rollout (Municipality + TSP + PDO) • Mesh topology for resilience **Phase 3: Access & Monetisation** • Free basic data (e.g., 100 MB/day) • Paid high-speed packs • Advertising integration **Phase 4: Trust & Awareness** • "TRAI Certified Secure Wi-Fi" tagging • Public awareness campaigns	Ensures sustainability, user trust, and measurable outcomes

Component	Detailed Analysis	Justification (Regulatory + Ground Reality)
	Phase 5: Monitoring • Real-time analytics dashboard (usage, QoS, uptime)	

B. INDOOR PUBLIC WI-FI (Controlled High-Density Spaces)

(Railway stations, airports, malls, institutions)

Structured Policy Evaluation Table

Component	Detailed Analysis	Justification (Regulatory + Ground Reality)
Problem Definition	• Fragmented Wi-Fi networks (no interoperability) • Poor QoS in peak hours • Repeated login inconvenience • Lack of standardisation across venues • Limited monetisation innovation	TRAI highlights need for better authentication, QoS, and interoperability frameworks
Possible Solutions	1. **Centralised Wi-Fi Management Platforms** 2. **Hotspot 2.0 / Passpoint (auto-authentication)** 3. **QoS-based bandwidth allocation** 4. **Neutral Host Wi-Fi Model** 5. **Integration with Digital Public Infrastructure (UPI, Aadhaar login optional)** 6. **Enterprise-grade SLA-based deployment**	Matches global best practices and high-density indoor requirements (airports, malls)
Evaluation of Options	• **Centralised control** → Improves performance & monitoring • **Passpoint** → Eliminates login friction (high adoption impact) • **QoS frameworks** → Essential for video/AR/IoT use cases • **Neutral host model** → Maximises infrastructure sharing • **DPI integration** → Simplifies authentication • **SLA enforcement** → Ensures service quality	Indoor environments require carrier-grade reliability as highlighted in the consultation
Judgement (Best Strategy)	**Carrier-Grade Managed Wi-Fi + Seamless Authentication + Neutral Host Model**	Ensures scalability, quality, and user convenience

Component	Detailed Analysis	Justification (Regulatory + Ground Reality)
Execution Framework	**Phase 1: Standardisation** • Mandatory Passpoint compliance • Unified SSID across public venues **Phase 2: Deployment** • Star/tree topology (as per venue size) • Fiber-based backhaul (preferred) **Phase 3: Service Model** • Free basic access + premium tiers • Enterprise partnerships (retail, ads) **Phase 4: QoS Enforcement** • Minimum speed standards • Congestion management policies **Phase 5: Integration** • Link with DigiLocker, UPI, public services	Aligns with TRAI's focus on high-capacity, reliable broadband environments

C. ROLE OF GOVERNMENT – FUNDING DEPLOYMENTS

Structured Policy Decision Table

Component	Detailed Analysis	Justification
Problem Definition	• Low ROI for private players (especially rural/outdoor) • High initial capex • Uneven deployment (urban bias) • Weak participation of local bodies	TRAI identifies low commercial viability and limited state/local participation
Possible Funding Models	1. **Viability Gap Funding (VGF)** 2. **PPP Model (Centre-State-Private)** 3. **Municipal-owned infrastructure leasing** 4. **Universal Service Obligation Fund (USOF)** 5. **Voucher-based model (EU WiFi4EU type)**	Based on global examples (EU vouchers, South Korea PPP model)
Evaluation of Options	• **VGF** → Most effective for rural/outdoor viability • **PPP** → Balanced risk sharing • **Municipal model** → Fast deployment but needs capacity • **USOF** → Strong for inclusion but needs targeting • **Voucher model** → Simple but limited scalability	Hybrid funding models perform best globally

Component	Detailed Analysis	Justification
Judgement (Best Strategy)	**Hybrid Model: VGF + PPP + Municipal Asset Monetisation**	Combines financial sustainability with rapid deployment
Execution Framework	**Step 1: Policy Design** • Define priority zones (digital deficit + high footfall) **Step 2: Funding Mechanism** • 30–50% VGF support for outdoor/rural hotspots • Tax incentives for private investment **Step 3: Institutional Role** • Local bodies: provide sites & power • TSPs/ISPs: provide backhaul & operations **Step 4: Performance-based Disbursement** • Funding linked to uptime, usage, QoS **Step 5: Monitoring & Transparency** • National Public Wi-Fi Dashboard • Public reporting of performance metrics	Ensures accountability, efficiency, and scale

Q10. If the Government decides to provide financial support for the proliferation of Public Wi-Fi, which funding mechanisms would be most suitable for India? Should a uniform funding mechanism be adopted nationwide, or should differentiated funding mechanisms be used for rural, urban, and high-footfall areas? Please provide your response in detail with justification.

Comments :

Economic Rationale for Public Wi-Fi Support

Affordable, ubiquitous broadband has strong public-good aspects and positive network externalities that the private market alone fails to deliver in low-income or remote areas. India's Universal Service Fund (now the Digital Bharat Nidhi) explicitly acknowledges a "lack of business case" and market failure in underserved regions. Without subsidy, private operators will underinvest in

high-cost, low-ARPU zones. Public Wi-Fi also relieves congestion on cellular networks, improving overall QoS. For example, TRAI notes that grants and **viability gap funding** can "offset costs in low-revenue or high-cost areas, enabling inclusive and scalable Wi-Fi deployment". In short, public funding addresses the rural/urban digital divide and internalizes spillovers (education, e-governance, economic activity) that benefit society at large.

Comparative Evaluation of Funding Models

A mix of models can be tailored to location and purpose:

- **USOF/DBN grants:** The Universal Service Obligation Fund (USOF) has financed rural Wi-Fi pilots (e.g. ₹350 million for RailTel to install hotspots at 200 rural railway stations) and BharatNet fiber. It can fund broadband backhaul and access in unprofitable rural areas. USOF/DBN grants are best for **remote villages and underserved rural clusters**, where pure market builds are unviable.

- **Viability Gap Funding (VGF):** VGF subsidies (government covering part of CAPEX) suit large infrastructure projects that are marginally unprofitable. For example, India used VGF for BharatNet fiber rollout. In Wi-Fi context, VGF can make municipal or high-footfall projects (e.g. airport, railway station networks) attractive to private/PPP builders. TRAI explicitly endorses VGF as a tool for "sustainable Public Wi-Fi ecosystems" alongside PPPs. Use VGF in **high-investment zones** where business cases are weak (e.g. connecting fiber to busy transit hubs or building citywide mesh networks).

- **Corporate Social Responsibility (CSR):** CSR grants can catalyze local Wi-Fi projects. Companies can fund community hotspots or digital literacy

programs (e.g. village or school Wi-Fi) as part of CSR. The TRAI paper calls this a “community-led model” where initial funding “comes through CSR funds of corporations or Government or NGOs”. Such grants are best for **rural/tribal communities or social infrastructure** (schools, health centers) where private incentives are very low.

- **State co-funding:** State governments can match central funds or fund local projects from their budgets. Many states have started their own Wi-Fi initiatives. For example, Tamil Nadu’s 2017 “Amma Wi-Fi Zone” allotted ₹850 crore to build 50 free Wi-Fi zones (at beaches, bus stands, markets) across the state. State co-funding is effective for **areas where local priorities or co-benefits exist** (e.g. state education networks, tourism hotspots).

- **Public–Private Partnerships (PPP):** PPP models leverage private investment and speed. Municipal or state agencies build basic infrastructure (e.g. fiber ducts, poles), and private partners deploy/operate the Wi-Fi (often sharing revenue or earning advertising fees). Delhi’s Smart City fiber ducts (under a PPP) and Gurugram’s Smart City PPP are examples of using private capital in city networks. TRAI emphasizes PPPs for urban backhaul and hotspot rollout. PPPs fit **urban/metropolitan areas and transit corridors** where user density can generate some revenue or strategic value.

- **Municipal/ULB-led models:** Local governments themselves can build and operate networks. This often uses smart-city budgets or municipal bonds. Chennai Corporation launched 30-minute free Wi-Fi at 49 public spots (parks, bus stands, junctions) by equipping “smart poles”. Cities can provide right-of-way, power, fiber, and run hotspots or hire a contractor.

Such models suit **dense city centers or high-footfall public spaces** where civic reach and public service are high priorities.

- **Revenue-sharing models:** Hotspots can be funded through ad sales or shared revenues. For example, local businesses or venue owners offer space for routers; they earn ad or subscription revenues split with network providers. TRAI notes "revenue-sharing arrangements" (ads, services) among stakeholders as a monetisation model. This model suits **crowded urban environments** (malls, transit hubs) where advertising or premium service can generate income to sustain free or subsidized access.

- **Targeted subsidies for PDOs/PDOAs:** Under PM-WANI, small entrepreneurs (PDOs) run hotspots. Targeted subsidies (e.g. vouchers, equipment grants or discounted bandwidth) can help them invest. For instance, TRAI already mandated that ISPs sell broadband to PDOs at no more than twice consumer tariffs, effectively lowering operating costs. Additional grants or procurement of routers (like one-time capital subsidy to buy Wi-Fi access points) could stimulate **rural and peri-urban PDOs** where profitability is weakest.

Each funding tool can be matched to geography: USOF/VGF and rural PSU projects in remote areas; state/state-UT agencies and CSR in lagging districts; smart-city PPPs and municipal models in cities; and revenue/advertising approaches at tourist sites, airports, stadiums. TRAI itself advocates **"differentiated frameworks for rural, urban, and high-footfall areas"**, reflecting this plurality.

Uniform vs Differentiated Funding

A one-size-fits-all scheme would be inefficient. Uniform subsidies risk overfunding easily served markets while neglecting truly needy regions. By contrast, **differentiated funding is economically and operationally superior**. Subsidies and grants should be concentrated where costs are highest and user ability to pay is lowest (deep rural, hilly terrain, small towns). In cities and affluent areas, private investment or light touch (e.g. PPPs, municipal provision) can cover much of the cost. TRAI notes the need for **targeted** deployments rather than blanket coverage. For example, using USOF/DBN grants to extend fiber to villages, while letting mobile providers and venue owners bear most urban deployments, conserves scarce funds. A differentiated approach also streamlines administration: district-level RoW committees and state-level PDOA schemes (as recommended by TRAI) ensure local conditions guide fund use. In sum, targeted funding yields higher "bang for buck" and flexibility, whereas uniform schemes dilute impact and invite waste in profitable zones.

Consumer-Centric Benefits

From a consumer viewpoint, funded public Wi-Fi greatly enhances affordability, quality, and access:

- **Improved Affordability:** Public Wi-Fi is far cheaper per GB than cellular data. In India, mobile broadband costs ~₹8.18/GB on average, while fixed/Wi-Fi is only ~₹0.28/GB. Thus even modest subsidies yield large savings for users. Free or low-cost hotspots (e.g. in village panchayats or bus stations) enable poor households to use data-hungry services (video lectures, telemedicine) without straining their budget.

- **Higher Quality of Service:** Public Wi-Fi, especially when well-engineered, can offload peak traffic from overloaded mobile cells. As TRAI notes, free Wi-Fi in dense areas "can serve as a cost-effective, high-capacity solution, particularly in high-footfall locations...offloading traffic from mobile networks". Less congestion means higher speeds and reliability for everyone. Moreover, funding can ensure adequate backhaul (fiber/satellite) for hotspots, preventing the bottlenecks seen in purely commercial setups.

- **Expanded Access for Key Groups:** Subsidized public Wi-Fi especially benefits **students, gig workers, small businesses, and rural users**. TRAI observes that Wi-Fi is "particularly relevant for low-income users, students, [and] small businesses" who need high data at low cost. For example, students can access educational content (online classes, e-libraries) in villages; delivery drivers or rural entrepreneurs can use hotspots for payment apps and customer calls. One study noted families no longer need to gather in public for connectivity – children can study at home once village Wi-Fi is available. Overall, funding public Wi-Fi directly furthers inclusion: it brings digital services (tele-education, UPI payments, e-govt) to the underserved at prices they can afford.

Industry Structure and Sustainability

Funding mechanisms shape the telecom ecosystem:

- **PDO Viability:** Grants and subsidies can make Public Data Office (PDO) businesses viable. For instance, TRAI's 2025 order capping broadband tariffs for PDOs ensures their costs stay low. Additional funding (e.g. capital grants for routers) would further improve margins for village ISPs.

Without support, many PDOs would shutter due to high fiber costs and meager revenues. Funding can thus seed a sustainable micro-ISP layer, critical for PM-WANI's decentralized model.

- **Incentives for ISPs:** Well-deployed Wi-Fi helps telecom companies too. Industry analysts warn that Wi-Fi offloading "will become an operational necessity" for carriers as 5G densifies and data use grows. By reducing congestion and deferring expensive spectrum/cell upgrades, public Wi-Fi offers indirect benefits to operators. If government funds extend networks into new areas, ISPs gain fresh customer bases. PPPs and revenue-share deals also align ISP incentives: a shared-cost model (e.g. carrier installs backhaul fiber for Wi-Fi hotspots) can be profitable if public demand is sufficient. Thus, targeted funding can actually **complement** ISP strategies rather than compete with them.

- **PM-WANI Ecosystem:** Sustained funding supports the PM-WANI architecture's growth. Government backing (via cheaper broadband, grants, or CSR tie-ups) encourages more PDOAs to register and aggregate Wi-Fi operators. This enlarges the ecosystem for consumer choice and scale. Conversely, lack of funding risks fragmentation: insufficient incentives for aggregators or spotty backhaul will leave many hotspots off-grid. Thoughtful subsidies ensure the PM-WANI network expands in a balanced way, rather than stalling mid-rollout.

Technology-Neutral and Forward-Looking Framing

Funding schemes should remain technology-neutral and future-proof:

- **5G Offload & 6G Densification:** As 5G/6G networks roll out, public Wi-Fi will complement them. Policymakers should allow LTE/5G spectrum and

fixed infrastructure to be shared for Wi-Fi backhaul wherever possible. For example, spectrum in 2.3/2.5 GHz can carry rural broadband, or 5G small cells can be dual-purposed for public Wi-Fi. Funding should not favor one access tech; rather it should boost **digital infrastructure capacity** generically. In dense cities, planning for 6G-era ultra-dense coverage implies more access points – funding might support urban backhaul (fiber/satellite) that is usable by any RAN (LTE/5G/Wi-Fi).

- **Fiberization Gaps:** The biggest bottleneck is often lack of fiber to the hotspot. India's BharatNet has extended fiber to ~2.18 lakh gram panchayats, but last-mile distribution is poor. International practice (and TRAI's analysis) shows governments prioritizing **backhaul-first** deployment. Thus funding should focus on extending fiber/ducts/satellite to street level, rather than only buying Wi-Fi routers. E.g. grants for "fiber to the lamppost" or subsidies for satellite backhaul can enable future-proof networks.

- **Neutral-host Models:** Singapore's Wireless@SG (nationwide public Wi-Fi) offers a template: the government built the backbone and let multiple private operators share it. India can mimic this by encouraging neutral-host deployments (one entity builds infrastructure, many operators rent capacity). Funding can underwrite the neutral host's capital costs, while operations are run competitively. This "access as a utility" approach is tech-agnostic: whether through Wi-Fi, 5G unlicensed, or future standards, a neutral-host backbone enables seamless connectivity.

- **Satellite Backhaul:** For the most remote hamlets and islands, satellite can substitute fiber. Funding should not exclude novel solutions: e.g. grant pilots for LEO/MEO satellite backhaul to village Wi-Fi points. Indeed,

India's own satellites are already used in the GESAC program to reach 17k community sites. A technology-neutral fund could allow both terrestrial and space links as viable backhaul, chosen per context.

In all cases, funding mechanisms (tax breaks, grants, VGF) should be open to any last-mile technology that serves the goal of wide, affordable connectivity.

International Best Practices

We can draw lessons abroad:

- **EU – Backhaul-First Broadband:** The EU provides extensive grants for fiber/backhaul before Wi-Fi. For example, European Structural and Investment Funds (ERDF) give non-repayable grants for broadband deployment, and the Rural Development Fund (EAFRD) co-funds rural broadband projects. These funds target ducts and fiber links, ensuring hotspots connect to robust networks. The WiFi4EU program even pairs municipal hotspot vouchers with guaranteed backhaul funding. India should emulate this "fiber-first" mindset: use USOF/DBN and state budgets to lay rural fiber, then plug Wi-Fi into it.
- **Singapore – Neutral-Host Wi-Fi:** Singapore's Wireless@SG is a government-backed Wi-Fi network covering nearly all public spaces. Crucially, its fiber backbone is shared by multiple ISPs "for regional zones to make deployment manageable". The iCELL/Firetide case study highlights planning and multi-operator collaboration. This neutral-host model kept deployment costs down and service quality high. India can adopt a similar approach for metros: e.g. municipal Wi-Fi infrastructure that any PM-WANI aggregator or ISP can use, funded by a mix of public grants and operator PPP.

- **Brazil – Targeted Hotspot Subsidies:** Brazil's "Wi-Fi Brasil" (through the GESAC program) installs free broadband in "socially vulnerable" locations (schools, remote communities, public squares). As of 2022, it had ~17,000 active Wi-Fi points (urban and rural), all provided free via satellite or terrestrial links. This targetted subsidy (zero tariff for users, fully funded by government) shows how concentrated investment in hotspots lifts inclusion. India could replicate this by subsidizing operators to provide free Wi-Fi in a defined set of community anchors (e.g. panchayats, health centers).

- **Indonesia – Village-Fund Connectivity:** Indonesia empowers villages to finance connectivity via the Dana Desa (village fund) program. In one case study, Bobong village used ~Rp 254M (~$15K) from its village budget to build a local ISP (a village-owned enterprise). The community plans to reinvest 20% of its annual village fund into expanding the network. Government guidance (from the Ministry of Villages and Digital Affairs) and regulations allowed this model to flourish. This shows that well-targeted grants to local governments – or even allowing villages to use existing development funds for Wi-Fi – can rapidly extend access. India's Gram Panchayat grants (or schemes like MGNREGA margins) could similarly support micro-ISP projects.

Recommended Hybrid Funding Approach

We propose a balanced, geography-sensitive hybrid:

- **Rural Areas:** Heavy reliance on **USOF/DBN grants and VGF** for backhaul and major equipment. For example, co-fund fiber and Wi-Fi deployment from GP to habitations (via BharatNet Udyamis or franchises). Use

targeted **voucher-like subsidies** for PDOs (especially in distant hamlets) so that local entrepreneurs can afford routers and satellite links. Encourage state governments to add matching funds (as some have done for rural broadband). NGOs/CSR can seed community Wi-Fi (e.g. at schools, panchayats) under a performance-linked grant.

- **Urban/City Areas:** Lean on **municipal and PPP** models. Cities should streamline RoW and street-light access (as TRAI suggests) to cut costs. Smart City or municipal budgets can finance fiber backbone to city centers. Private operators (TSPs/ISPs) should deploy the access points, possibly under competitive tenders or bundled with civic services. Revenue-share/ad models can support free Wi-Fi in markets, bus depots, tourist spots. Minimal central grant (or small VGF) may be used for "last 10%" coverage of underserved pockets.

- **High-Footfall Locations:** Use **PPP and targeted subsidies**. For transit hubs (airports, stations, stadiums), governments can tap CSR and tourism boards, or strike concession deals (e.g. contracted operator shares ad/profit). In tourist corridors, subsidies (even small ones) encourage operators to offer free Wi-Fi in return for marketing. Performance-linked grants (e.g. pay per user) could be piloted.

- **Integrated State Programs:** States/Uts should act as aggregators/beneficiaries. As TRAI notes, state agencies (like TN-CIT or MPSEDC) could become PDOAs, pooling efforts. States can then use their budgets or SASCI loans (or CSR quotas) to fund expansion in their territory, complementing USOF. This dual funding (centre+state) ensures alignment with state priorities.

In sum, **no single mechanism suffices**. We advocate a layered model: central USOF/DBN for wholesale infrastructure, state/local and private funds for distribution, CSR/community funds for last-mile innovation, all under the guiding principle of coverage equity.

Phased Implementation Roadmap

A staged rollout can manage complexity:

1. **Year 1–2 (Preparation and Pilots):** Conduct granular surveys of backhaul gaps (fiber and wireless) and user demand. Simplify regulations (RoW, single-window permissions). Select pilot districts: one tribal/rural, one tier-2 city, one mega-city. Deploy differentiated funding: e.g. pilot USOF-funded Wi-Fi networks in blocks lacking broadband, PPP-driven Wi-Fi in a smart city area, CSR-sponsored hotspots in select panchayats. Establish institutional structures (district RoW cells, state PDOAs). Begin IEC campaigns to register PDOs.

2. **Year 3–4 (Scale-up and Integration):** Evaluate pilots, refine models. Scale successful rural schemes (BharatNet+Wi-Fi bundles) to adjacent districts. Expand urban PPP networks into more cities. Incorporate 5G offload by co-locating APs on 5G towers. Introduce targeted subsidies for PDOs in low-coverage census blocks. Roll out schemes like WiFi4EU-style voucher to tier-2 towns. Use SASCI loans (as TRAI suggests) to expand state fiber grids. At this stage, monitor QoS metrics and adjust funding per ROI.

3. **Year 5+ (Optimization and Future Tech):** Transition some grants to performance-based (awarding funds for meeting speed/uptime targets). Leverage new tech: pilot satellite backhaul in island/remote areas. Integrate with future smart infrastructure (IoT sensors on Wi-Fi poles).

Prepare for 6G trials (dense small-cell and Wi-Fi convergence). Evaluate financial sustainability: gradually shift mature urban zones to market funding as usage grows. Conduct impact assessment on inclusion (student access, rural livelihoods) to inform future budgets.

Throughout, maintain a **cross-cutting focus** on capacity building (training PDOs, digital literacy for users) and consumer protection (affordability, data privacy). Regularly review and reallocate funds per area needs; TRAI's suggested committees and municipal assets can aid coordination.

In conclusion, a hybrid funding architecture – combining USOF/DBN, VGF, CSR, state and municipal inputs, and PPP arrangements – tailored by geography, will economically justify public Wi-Fi expansion while ensuring consumer benefits. This balanced, phased strategy draws on both domestic priorities and global best practices to sustainably bridge India's connectivity divide.

Mechanism	Best fit	Capital vs Opex	Pros	Cons
USOF / BharatNet linkage	Rural, remote villages	Capex heavy	Leverages existing BharatNet backhaul; proven rural reach.	Slow rollout; needs O&M plan.
Viability Gap Funding (VGF)	Pilot/difficult rural & social sites	Capex + limited Opex	Makes socially desirable but unviable projects bankable.	Requires strong project appraisal; fiscal limits.
PPP / Municipal co-funding	Urban public spaces, transit hubs	Capex + Opex sharing	Local ownership; faster deployment; aligns with ULB priorities.	Coordination complexity; variable ULB capacity.
Revenue-share / commercial models	High-footfall commercial hotspots	Opex recovery	Market sustainable; incentivises	May underserve low-income users without subsidies.

Mechanism	Best fit	Capital vs Opex	Pros	Cons
			quality and uptime.	
CSR / Philanthropy / Grants	Targeted social use (schools, health)	Capex or Opex	Flexible; quick deployment for social objectives.	Not scalable as sole source.

Q11. What criteria should govern the allocation and disbursement of funds across rural, urban, and high-footfall areas, respectively? Please provide your response in detail with justification. C. Role of Government- Backhaul provisioning and funding

Comments :

Funding Allocation Framework for Public Wi-Fi in India

Guiding Principles: Public Wi-Fi funding should follow principles of equity, efficiency, sustainability and consumer protection. Funding must target the digital divide (equity) by prioritizing underserved populations and areas with low broadband penetration. It should maximize impact per rupee (efficiency) by filling market gaps rather than subsidizing already-viable markets. Sustainability requires clear O&M plans and performance links, so that funded hotspots continue operating. Finally, consumer protection demands affordable service (free or low-cost tiers), minimum quality standards and safeguards against hidden costs or data caps. In short, we treat broadband access as a quasi–public good: it generates strong positive externalities (education, health, commerce) that the private market alone undersupplies, justifying well-targeted public support.

Criteria for Geography-specific Funding: We propose distinct criteria for rural, urban, and high-footfall locations, each reflecting their needs and usage patterns:

Rural areas: Prioritize places that are unserved or underserved by 4G/5G and fiber, far from existing PoPs, with very low broadband take-up. Metrics include distance to BharatNet fiber nodes, absence of backhaul, village income levels, school/clinic coverage and population density. Funding focus: areas with no private incentive to build. The socio-economic case is strong: Wi-Fi in village schools, panchayats, and clinics powers education, telemedicine and e-governance. Given sparse population and low ARPU, these projects typically need substantial capital subsidy or viability support. Government must ensure backhaul (e.g. extend BharatNet fiber or satellite links to remote gram panchayats) and consider grants or VGF for local Wi-Fi last miles. Institutional sites (schools, PHCs) should be anchor clients. Funding disbursement should favor projects that commit free or highly affordable service to villagers (for example, free basic tier for education/health and nominal fees for extra use) and meet strict QoS benchmarks (uptime, speeds) – only releasing funds as agreed milestones are met.

Urban areas: Criteria should identify pockets of need in otherwise well-served cities. Important dimensions include population density and vulnerability: areas with many students, migrant workers, low-income colonies or homeless populations who lack affordable broadband at home. Also include neighborhoods lacking any fixed broadband competition. Here the cost of rollout/backhaul is much lower (fiber is often nearby), so blanket subsidies are not needed. Instead, small targeted support (equipment

grants, rental concessions) can catalyze hotspots where market forces alone leave gaps. Government role is lighter: for example, city or state funds might co-finance Wi-Fi in municipal schools, libraries, or bus termini. Local administrations can mandate that public housing or transit projects include Wi-Fi. Affordability safeguards are crucial – e.g. sites must offer at least a free basic tier – but private operators can recover costs through paid upgrades or ads. In sum, urban funding is modest and strategic (filling blind spots for the needy) rather than wholesale.

High-footfall areas: These include railway stations, bus terminals, airports, tourist spots, markets, hospitals, large campuses and public venues. **Criteria here focus on daily footfall and usage type:** number of people served per day, nature of demand (commuters, patients, students, tourists), and public-interest value. Many of these sites have captive audiences and potential revenue (ads, sponsorships, premium services), so projects can often run as PPPs. Government funding should be *least* here, limited to where viability still falls short – for example, VGF to entice a private provider at smaller stations or rural helipads. Corporate CSR or grants have historically driven Wi-Fi at large stations and marketplaces, which is appropriate: e.g. major railway stations largely financed by PSU RailTel and CSR (as PMO data shows). In high-footfall zones, government can contribute by providing space and ducting free of charge (public assets), by allocating fiber backhaul where it exists, or by offering tax/advertisement incentives. But broad subsidies are rarely needed: most of these sites can attract private operators with minimal support.

Government's Backhaul and Funding Role: The central government's core role is to provide backbone infrastructure and capital support where the

market won't. This means expanding BharatNet and fiber deep into rural India as the common rural backhaul layer. States should use BharatNet fiber actively and support private "last-mile" extensions (e.g. through BharatNet Udyamīs who take fiber into villages). Government should also fund backhaul alternatives in the hardest places: satellite- and microwave-linked Wi-Fi hotspots (using programs like USOF or new funds) can serve very remote hamlets or islands. In cities, government can ease right-of-way and encourage shared underground ducts so fiber can reach Wi-Fi nodes in public spaces. Overall, public funding (through USOF or the new Digital Bharat Nidhi, etc.) must fill last-mile gaps; evidence suggests Wi-Fi is most cost-effective where mobile coverage is thin.

Funding Models and Geographic Fit. No single model suits all areas. The comparative fit is:

USOF / Universal Funds: Best for rural and remote areas. Traditionally financed rural wireline/broadband projects, and now can be repurposed to fiber + Wi-Fi grants. For example, USOF paid for Wi-Fi at 193 rural railway stations. Going forward, USOF/DBN funds should subsidize the capital costs of rural hotspots and backhaul in "no-go" zones.

Viability Gap Funding (VGF): Works well for PPPs where demand is moderate. Use VGF to encourage private Wi-Fi providers to set up in villages or towns that are not fully viable, or to upgrade infrastructure at key urban hubs. For instance, State Digital Networks or smart city PPPS can include VGF if use-cases benefit public services.

Corporate Social Responsibility (CSR): Ideal for high-footfall and civic spaces. Already seen at railway stations, bus stands, and tourist spots. CSR funds can build and operate hotspots in places like major stations and universities at little or no cost to government. These are one-off gifts rather than sustained O&M models, so CSR should be used to kickstart projects (especially where visibility is high) and attract footfall.

State co-funding: State governments can match central grants in areas of local priority. Wealthier states could co-invest in their own rural broadband or city-wide Wi-Fi, driving higher local buy-in. States may also tap schemes like the SASCI fund to get interest-free loans for digital infrastructure (subject to implementing reforms like RoW rules).

Public-Private Partnerships (PPP): Crucial for markets with some revenue potential (high-footfall urban and peri-urban). Examples include companies (or PSUs like RailTel, NM-ICIC) deploying Wi-Fi in exchange for ad revenues or user fees. PPP is best where footfall or business usage is strong; government can use asset transfers (e.g. existing ducts or towers) and minimal subsidies to attract private partners. Smart-city Wi-Fi projects are typically PPPs, often funded partially by city budgets or central grants with local execution.

Municipal/ULB models: Cities can run their own Wi-Fi, especially at public facilities (libraries, parks). While rare in telecom, some municipalities operate or contract free hotspots in public areas. Funding here often comes from local taxes/municipal budgets plus small state grants. This is more niche but can fill city-service gaps where private players won't bother (e.g. inner-city slums).

Revenue-sharing models: In high-traffic venues (malls, metro, airports), operators sometimes install Wi-Fi with the understanding that revenue from advertising, signage, or premium vouchers is shared with the site owner. This "no upfront subsidy" model works when a stable revenue stream exists. It fits high-footfall sites but not uneconomic rural spots.

Targeted PDO/entrepreneur subsidies: Under PM-WANI, individuals can become Public Data Office operators (PDOs). Targeted funds (small grants, free or discounted routers, training) for PDOs/PDO-aggregators (especially in villages and small towns) can spur grassroots deployments. For example, subsidizing Wi-Fi kit for shopkeepers in rural hubs can quickly boost hotspots at low cost.

Each model's suitability aligns with geography: e.g., USOF for villages, CSR and PPP for transit hubs, municipal funding for civic areas, etc.

Uniform vs. Differentiated Funding. A one-size-fits-all subsidy regime would be wasteful and inequitable. Uniform funding (for example, equal grants per site regardless of location) ignores the stark cost and demand differences between a Mumbai slum and an Odisha panchayat. It would overspend where private viability is high and undersupply where viability is low. In contrast, differentiated funding – allocating more support to hard-to-serve regions and less to self-sustaining areas – is both efficient and fair. TRAI itself recommends separate frameworks for rural, urban, and high-footfall zones. This allows high subsidies (e.g. full capex coverage) in rural sites with little user revenue, moderate subsidies (VGF) in semi-urban or smaller towns, and minimal grants in dense urban or gateway areas where commercial returns are better. In practice, this means rural Wi-Fi grants tied

to need and usage (e.g. more funds per unserved village), versus leaner assistance (like providing only site access or fiber) in well-connected cities. Such targeted allocation maximizes social benefit per rupee: it brings first-time connectivity to the last mile (bridging the digital divide) while ensuring public funds are not wasted on projects that would proceed anyway.

Consumer-Centric Impacts. The ultimate goal is expanded, affordable, quality internet access for all. Funding public Wi-Fi supports consumers directly: Wi-Fi can be offered cheaply or free, drastically lowering the cost of data (studies show per-GB Wi-Fi costs are much lower than mobile data). This is critical for low-income households, students and gig workers who are extremely price-sensitive. For example, community-funded Wi-Fi in a remote village enabled children to study at home instead of gathering outside for signal, illustrating how affordable Wi-Fi empowers education. Small businesses benefit too – in the same village, shopkeepers began using WhatsApp and e-payments, expanding their markets. Overall, better funding translates into more hotspots (greater **access**), stronger signals (better quality of service), and guaranteed free or tiered pricing (enhanced affordability). It closes rural-urban gaps: if rural health centers have Wi-Fi, telemedicine can reach patients; if Gram panchayats have it, citizens can access e-Gov services without traveling. By mandating non-discrimination and fair-pricing clauses in funded projects, the framework ensures no user is gouged on Wi-Fi networks.

Industry Viability and Sustainability. Sound funding boosts the long-term health of the Wi-Fi ecosystem. By covering initial capital costs and backhaul investment (especially via schemes like BharatNet), the government lowers barriers for Public Data Operators (PDOs). This makes their business viable

– they can cover modest operational costs through user fees or paid services on top of a free basic tier. Clear subsidy stages (e.g. grant, then partial cost-recovery) help PDOs plan sustainable operations. For ISPs and TSPs, a well-funded Wi-Fi layer is complementary, not cannibalistic: it offloads high-bandwidth traffic (video, downloads) from cellular networks, improving overall quality for mobile users. Indeed, TRAI notes that Wi-Fi offloading can defer costly spectrum upgrades and relieve congestion. Funding should therefore be designed to align incentives: for instance, mobile operators could be invited as PM-WANI aggregators who benefit from offload, or given incentives to link their infrastructure to community Wi-Fi. Importantly, funding should support the PM-WANI neutral-host vision: PPP grants and disbursement terms must not distort competition (i.e. avoid giving unfair advantage to one provider). Performance-linked funding (releasing payments only as usage and QoS benchmarks are met) will pressure PDOs and ISPs alike to operate reliably, fostering a robust, consumer-trusted Wi-Fi market.

Technology-Neutral and Forward-Looking Framing. The framework is technology-agnostic: support can be used for any practical connectivity solution. This means Wi-Fi funding goes hand-in-hand with 5G and future networks. For example, government-backed public Wi-Fi will help 5G networks by offloading data in dense urban cells (making 5G more efficient for mission-critical use). Conversely, as 6G approaches, it is expected to rely on ultra-dense deployments and possibly integrate unlicensed spectrum, so a strong Wi-Fi infrastructure will complement that future. Fiberization gaps are explicitly addressed by funding strategies: continued BharatNet expansion and support for private fiber builds ensure robust backhaul, which in turn boosts both Wi-Fi and cellular speeds. For truly remote areas,

supporting satellite backhaul (e.g. through Space Research funded ground stations or subsidies for BNG hardware) can link hot spots to the internet where laying cable is impossible. Neutral-host models (shared Wi-Fi infrastructure serving multiple providers) are encouraged – for instance, building shared in-building Wi-Fi in large complexes as part of building codes (as already recommended in TRAI's consultation). In sum, the funding approach does not pick winners among technologies but ensures any cost-effective solution — terrestrial or satellite, Wi-Fi or small-cell, state or private-run — can be financed if it meets the public-interest criteria.

International Best Practices. India's strategy can draw lessons from abroad. In the EU, many broadband subsidy programs stress "fiber first" for rural areas: grants typically require or prioritize upgrading backhaul before last-mile access, to ensure sustainable high speeds. Singapore's Wireless@SG is an example of a neutral-host public Wi-Fi system funded by the government and industry, providing thousands of free hotspots in malls, parks and transport hubs; this model ensures dense, interoperable coverage. **Brazil** has used targeted hotspot subsidies – the government funds free Wi-Fi in over 7,500 locations (serving social institutions and communities) as part of its national connectivity plan. Indonesia has subsidized rural connectivity by empowering local co-ops and village enterprises: for example, villages use state "Dana Desa" funds and central grants to build their own networks, proving that community-driven, government-backed projects can succeed (as seen in Taliabu's village Wi-Fi initiative). Each of these shows the value of coupling backhaul investment with local deployment incentives, and of tailoring solutions to local contexts – lessons directly applicable to India's differentiated approach.

Hybrid Funding Recommendation. No single instrument can cover all needs. The practical solution is a hybrid: one that blends central grants, loans, subsidies and private investment. For instance, combine USOF/DBN grants for rural backhaul and last-mile with VGF for semi-viable projects and CSR/municipal contributions for high-footfall sites. In rural block pockets lacking any infrastructure, governments would finance nearly 100% of capex (through USOF) to make Wi-Fi happen. In somewhat connected villages, VGF or state–user contributions can share costs. In cities and transit hubs, rely on PPP and CSR, with government only stepping in to reduce upfront barriers (e.g. free fiber or discounted power to encourage Wi-Fi). All funding should be outcome-linked: payments to any provider (PD/ PDOA) would be staggered based on rollout milestones, user uptake or uptime targets, ensuring accountability. This balanced approach targets scarce subsidy where it unlocks access, while letting market forces operate where feasible, achieving maximal coverage without wasteful spending.

Phased Implementation Roadmap. A phased rollout will ensure maturity and course-correction:

1. Phase I (Year 1): Assessment & Quick Wins. Map connectivity gaps using BharatNet/rollout data and local surveys. Identify priority “pilot” sites (e.g. largest unserved villages, busiest transit hubs). Launch Wi-Fi in a handful of Gram Panchayats and major stations under mixed funding (USOF + CSR/PPP). Simultaneously, establish performance monitoring systems, QoS standards, and grievance mechanisms.

2. Phase II (Years 2–3): Scale Rural Backhaul & Catalyze Hotspots. Expand BharatNet deeper (using USOF/DBN) to cover backward blocks. Fund satellite links or microwave to hardest areas. Roll out PDO/PDOA subsidies

across rural India (small grants for shopkeepers, CSC expansions). In parallel, continue deploying Wi-Fi at schools, PHCs, panchayat offices via state–center co-funding. Urban pilot projects launch: e.g. Wi-Fi at bus depots or community centers using municipal funding + CSR.

3. Phase III (Years 4–5): Expansion & Optimization. Analyze early results, refine criteria (e.g. adjust subsidy levels based on demand). Increase funding to successful areas and phase out in areas now commercially viable (for example, remove subsidies in towns where many paid users emerge). Begin integrating Wi-Fi planning with 5G/6G networks (ensuring offload use). Support evolution of neutral-host in-building Wi-Fi in new developments. Promote private innovation: e.g. challenge grants for new Wi-Fi business models.

4. Ongoing: Continuous improvement. Each year, reallocate resources to new white spaces and measure social impact (internet adoption rates, digital inclusion indices). Update criteria as technology and usage change (for instance, raising speed targets as broadband expectations rise). Ensure transparency: all funding schemes publish disbursements, usage stats and audits. By this roadmap, funding flows adapt from heavy initial support to eventual sustainable operations, with government stepping back as local markets mature.

In summary, the policy calls for a criteria-driven, geography-specific financing framework for public Wi-Fi. It aligns subsidy with actual need (connectivity gap, socio-economic factors, backhaul availability) and links disbursement to performance. Rural schemes will lean on BharatNet and USOF/DBN, urban gaps will see modest targeted support, and high-footfall sites will be tackled via PPP/CSR and selective funding. Consumer-centric

safeguards (affordability, QoS metrics, open-access rules) are built into the criteria. This hybrid, phased approach leverages multiple funding models and global lessons to ensure that every Indian – student, farmer, worker or entrepreneur – gains affordable, reliable internet access, without propping up unsustainable services.

Q12. Is the lack of adequate and reliable last-mile connectivity a critical constraint for the proliferation of Public Wi-Fi in the country? If yes, what specific measures may be considered by the Central Government, State Governments, and local bodies to address the last-mile constraints? Please provide your response in detail with justification.

Comments : No Comments.

Q13. Is there a need for the Government to provide funding for provisioning of last mile connectivity in the uncovered or underserved areas for Public Wi-Fi networks? If yes, which funding option is best suited in the Indian context, and what should be the criteria for rural, urban, and high footfall areas, respectively? Please provide your response in detail with justification. D. Facilitative role- States and local bodies

Comments : No Comments.

Q14. Are there any RoW challenges faced by service providers in accessing public places or street furniture to install Public Wi-Fi hotspots? If yes, details may be provided along with suggestions for improvements. Please provide your response in detail with justification.

Comments : No Comments.

Q15. What facilitative roles can State Governments play in accelerating Public Wi Fi deployment across rural, urban, and high-footfall areas, respectively? Should States consider deploying Public Wi-Fi networks at the municipal and gram panchayat level? Please provide your response in detail with justification.

Comments : No Comments.

Q16. Should the State Government need to take initiatives to improve the availability of last-mile connectivity for Public Wi-Fi networks? If yes, what measures can incentivise States /municipalities to undertake city- and town level fiberisation to ensure Public Wi-Fi network proliferation? Please provide your response in detail with justification.

Comments : No Comments.

Q17. What facilitative roles can local bodies play in accelerating the deployment and sustainable operation of Public Wi-Fi networks in rural and urban areas? Please provide your response in detail with justification. E. Incentivising Service Providers

Comments : No Comments.

Q18. What regulatory or policy incentives, schemes or programs are required to promote active participation of TSPs and ISPs in Public Wi-Fi deployment? Please provide your response in detail with justification.

Comments : **No Comments.**

Q19. What regulatory or fiscal incentives, schemes or programs may be required in the provisioning of bandwidth and backhaul for Public Wi-Fi networks? Please provide your response in detail with justification. F. Incentivising Private entities

Comments : **No Comments.**

Q20. What measures can be adopted to incentivise private enterprises, commercial establishments, shop owners, community institutions etc. to install public Wi Fi hotspots? Please provide your response in detail with justification.

Comments : **No Comments.**

Q21. Is there a need to strengthen the role of public or private entities as system integrators for the deployment of Public Wi-Fi networks? If yes, what policy or institutional support may be required? Please provide your response in detail with justification. G. Technical Architecture, Authentication, and Interoperability

Comments : **No Comments.**

Q22. Are users facing challenges in the authorization and authentication procedures for accessing Public Wi-Fi Networks? If yes, how can authorization and authentication processes be simplified while

ensuring security and compliance? Please provide your response in detail with justification.

Comments : No Comments.

Q23. Is there a need for a centralized platform for authentication and payment systems in the Public Wi-Fi ecosystem? If yes, which entity is best suited for its implementation and management? Please provide your response in detail with justification.

Comments : No Comments.

Q24. What steps are required to achieve interoperability and seamless roaming among Public Wi-Fi networks? Should inter-hotspot roaming be made mandatory, and if yes, should a "super-aggregator" need to be introduced to facilitate it? Please provide your response in detail with justification. H. Monetisation and Sustainability

Comments : No Comments.

Q25. What monetisation models are most appropriate for rural, urban, and high footfall locations, respectively? Please also suggest any additional monetisation models that may be suitable in the Indian context. Please provide your response in detail with justification.

Comments :

Monetisation Models for Public Wi-Fi: Rural, Urban and High-Footfall Areas:

To ensure the sustainability of India's PM-WANI public Wi-Fi ecosystem, appropriate monetisation models must balance financial viability with universal access. Public Wi-Fi networks generate social benefits (education, health, governance) that private markets undersupply. Differentiated models are therefore needed by geography: rural areas with low income and sparse demand require subsidy and public support, while dense urban zones and busy public venues can leverage advertising and paid tiers. Importantly, any monetisation strategy must preserve consumer affordability and quality-of-service – free or very low-cost basic access must be guaranteed for underserved users even as premium services are monetised.

1. Policy Context: Monetisation & Sustainability

Public Wi-Fi drives digital inclusion, but needs revenue or subsidies to be sustained. In isolation, rural hotspots often lack paying users and face high backhaul costs, while urban/high-traffic hotspots can attract more users and fees. Monetisation must therefore be layered: a base level of free or low-cost access to meet the equity and affordability goals of Digital India, with higher-speed or value-added services generating revenue. TRAI's consultation and international practice note that viable Wi-Fi deployments use a mix of direct (user fees, freemium) and indirect (advertising, sponsorships, data services) models. Globally, successful public Wi-Fi (e.g. UK's networks) rely on free-to-user access subsidised by adverts and sponsorships. In India, monetisation must also promote mobile offload benefits and data analytics opportunities that accrue indirectly (for example, easing mobile network congestion).

2. Geography-Wise Monetisation Strategies

A. Rural Areas

Rural India presents low commercial viability: incomes are low, willingness to pay is limited, and users are dispersed. On metrics, urban internet penetration (~112%) far exceeds rural (~45%), indicating a persistent affordability gap. Government support is therefore essential. Key models include:

Government-Funded Backhaul + Free/Low-Cost Access: Extend BharatNet fiber or satellite backhaul to villages, and attach Wi-Fi hotspots at gram panchayats, schools, PHCs, PDS outlets etc. These Wi-Fi access points should offer a free basic tier (e.g. a daily free allowance of data) to ensure connectivity for all. This addresses the market failure by injecting capital: universal service funds or new grants can underwrite the high fixed costs of rural backhaul. Even if the hotspot operates at a loss, the social returns (education, e-services) justify subsidy. For example, India's RailWire model provides free Wi-Fi (e.g. 30 min at 1 Mbps) at 6,000+ stations (most in rural areas), illustrating that free basic service can be sustained with support and optional paid upgrades.

Viability Gap Funding (VGF) for PDOs/PDOAs: The government can offer VGF or revenue guarantees to Public Data Office aggregators (PDOAs) or operators (PDOs) in remote areas. Analogous to past telecom rural subsidies, VGF would cover part of the shortfall, ensuring that local entrepreneurs are not left with zero margin. For instance, a village Wi-Fi operator might receive a monthly subsidy or be guaranteed a minimum per-hotspot income. This conditional support ("pay-for-performance" grants) can be tied to coverage/milestone metrics to avoid waste.

Community-Driven Wi-Fi (CSR/NGO Partnerships): Harness local entrepreneurship and community groups. Non-profits, cooperatives or even micro-entrepreneurs (e.g. shopkeepers, teacher groups) can run "Wi-Fi shakti kendra"-style hubs. Initial capex (routers, power backup) can come from CSR funds, NGOs, or local government grants, with the community sharing operation costs. In this model, revenue need not come from end-users but from advertising or sponsorship. For example, a village hotspot near the Panchayat office might display local ads or government announcements (supported by CSR), making it effectively free to users. Community ownership also encourages sustainability (community members have a stake in maintenance).

CSR-Funded Social Hotspots: Companies' CSR programs can be directed to public Wi-Fi deployment in rural schools, PHCs, libraries, and transit hubs. Models like "digital literacy hubs" funded by corporate grants have precedent. These hotspots, operated by NGOs or vendor partners, would provide free or nominally priced access with educational content – a public good. For example, Coca-Cola and Intel have sponsored village Internet cafes in the past. Targeting such CSR funds to Wi-Fi expands access at no cost to users.

Subsidised Satellite-Backed Wi-Fi: In extremely remote/tribal areas where fiber is impractical, leverage satellite connectivity as backhaul (e.g. via VSAT or LEO services). Hotspots could then be established at key community points. Government or CSR subsidies would keep user charges minimal. Though more expensive, satellite Wi-Fi can fill the last gap in "islands" of no connectivity. Policy support (discounted spectrum, grants) can make such service affordable.

Justification: These models combine to address rural needs. They align with universal service principles: subsidise where markets under-provide. Social benefits are high (e.g. supporting remote education and healthcare), so subsidising free basic access improves equality. Meanwhile, community or CSR involvement reduces the fiscal burden and increases local buy-in. Such composite models have worked elsewhere: the Broadband India Forum notes community entrepreneurs can profitably add services around local Wi-Fi, and TRAI's consultation highlights Community-led (CSR/NGO) funding as a viable model.

B. Urban Areas

Cities and towns have mixed viability. Urban hotspots see higher footfall and more users with ability to pay, but also expensive real estate and competition from home broadband/mobile data. Monetisation in urban areas should tap density and diversity:

Freemium Model: Provide a basic free tier (e.g. limited data/speed per day) and premium paid tiers for greater speed or volume. This encourages adoption by all, with revenue from those needing more. For instance, a public park or college campus could offer students free low-speed Wi-Fi for classwork but sell higher-speed plans to professionals. TRAI notes freemium works well in institutions and transport hubs. The free tier ensures inclusion (students, low-income citizens), while the paid tier attracts those who can pay (business users, tourists).

Advertisement-Sponsored Access: Urban hotspots (especially malls, metros, markets) can be free for users in exchange for viewing ads on the login page or receiving promotional content. Advertisers value urban footfall; for example, a mall could sell ad space on its captive portal to local

shops or brands. TRAI highlights advertising as effective in high-footfall spaces. In cities like Bengaluru, free Wi-Fi zones have successfully run on local sponsorships. Bundling with Digital India's Open Platform (e.g. displaying civic messages) can also leverage public information.

Municipal/ULB Co-funded Hotspots (PPP): City governments or Smart City agencies can co-invest in Wi-Fi infrastructure in underserved neighbourhoods (e.g. slums, low-income areas). Under a PPP, the local body provides right-of-way or partial funding (fiber, poles), while private operators install and run hotspots. For example, municipal broadband projects in other countries (Austin City Wi-Fi, Bangalore's Namma WiFi) combine taxpayer funds and private management. Co-funding lowers risk for providers and ensures coverage in areas they might otherwise avoid, while cities gain e-government penetration and citizen services.

Neutral-Host/Infrastructure Sharing: Urban densification makes multiple separate networks impractical. A neutral-host model (single shared network serving all) can be used, especially in transit zones or campus environments. Under this model, multiple ISPs or TSPs co-invest in a common Wi-Fi infrastructure (or backhaul towers) to offload mobile traffic. Singapore's Wireless@SG is a federated model where ISPs and venue owners share infrastructure. In India, this could mean a tower or optical node serving multiple "PayFix 3.0" hotspots. Neutral-host reduces duplication, lowers O&M costs, and enables unified plans; for example, a metro rail could allow carriers to use its Wi-Fi under revenue-share.

TSP-Bundled Wi-Fi: Encourage mobile operators to bundle Wi-Fi passes in their data plans (as is common in many markets). Customers paying for postpaid or prepaid plans get free Wi-Fi access at PM-WANI hotspots. This

provides an indirect revenue model: carriers offload busy cell sites, and hotspots gain captive traffic. Such bundling is noted by TRAI as a monetisation strategy. In practice, an ISP might subsidize hotspot deployments by regional cable operators or broadband ISPs, in exchange for including those hotspots in their own 5G/4G data plans.

Justification: Urban populations are heterogeneous. High densities and commercial venues support business models, but significant sections (students, migrants, low-income families) need free or low-cost access for school, job search and services. Freemium and ad models capture surplus without excluding the poor. Municipal co-funding and neutral-host frameworks leverage public infrastructure for public benefit. Overall, these urban models mix revenue-generation with subsidy intelligently, unlike a blanket "pay all" approach which would curb inclusion.

C. High-Footfall Locations (Transport Hubs, Markets, Campuses)

Busy public spaces can often sustain commercial Wi-Fi due to huge user numbers. Their monetisation can be aggressive yet consumer-friendly:

Paid Tiered Access: In airports, stations or malls, premium paid plans (e.g. time-based or data-based passes) are viable since many users highly value connectivity (e.g. business travelers, tourists). For example, Indian RailTel's Wi-Fi at stations offers the first 30 minutes free and then sells daily/monthly packs. Similarly, airports often sell faster/high-cap plans. These paid offerings can be priced modestly (e.g. ₹10 for 5 GB), but cumulatively generate stable revenue given high traffic.

Revenue-Sharing with Venue Owners: Hotspot providers can partner with venue owners (e.g. stadiums, markets, schools) under revenue-share deals.

The venue might let the provider install equipment at low or no cost in exchange for a cut of ad or subscription revenue. This aligns incentives: the owner's interests (attracting visitors) are met while the provider sells access. Many stadiums or amusement parks worldwide use this model: visitors use free Wi-Fi, monetised by venue branding and a share of any data sales.

Sponsored Wi-Fi: Corporate sponsorship can underwrite high-traffic hotspots. For instance, a commuter plaza might have Wi-Fi "powered by" a brand or even financed by an OTT or fintech startup seeking customer eyeballs. The sponsor's logo appears on the login page in exchange for funding the service. Such sponsored models are common abroad and emerging in India (some cafes sponsor free wifi to draw customers). Importantly, sponsors must not lock content (all sites should be open as per PM-WANI principles).

Data Analytics and Services: High-footfall hotspots can sell aggregate, anonymised footfall/usage analytics to businesses (e.g. mall retailers, transit authorities). For example, a metro Wi-Fi could offer retailers data on how many commuters enter certain areas at peak times. While not a direct Wi-Fi charge, this **indirect monetisation** increases the venue's revenue, justifying investment in the hotspot. It is crucial to protect privacy (only aggregate, opt-in data) but such intelligence is valuable for advertisers and planners.

Value-Added Bundles: Tie Wi-Fi access to other purchases. For example, a concert ticket or airline boarding pass could include Wi-Fi code; bus/metro smartcards could store Wi-Fi vouchers. This both promotes usage and can be monetised through partnership (e.g. bundling deals with transport operators).

Justification: High-traffic sites host users with urgent connectivity needs and some payment ability, so **commercial models** make sense. Offering premium paid tiers captures that revenue. Venue partnerships and sponsorships lower the provider's costs and expand reach. Meanwhile, providing even a free basic tier keeps the service aligned with public benefit (e.g. patients in a hospital using email). Ultimately, monetisation here is not at odds with access – free Wi-Fi is a draw, and paid/sponsored enhancements make it sustainable.

3. Additional India-Specific Models

Beyond the above, innovative models can be tailored to India's context:

Digital Payments Incentives: Integrate Wi-Fi usage with India's digital payments ecosystem. For example, users who pay for Wi-Fi via UPI or BHIM apps could receive cashbacks or discounts on bills. This encourages formal payment and can be co-funded by fintech promotional budgets. Conversely, e-wallet loyalty points could be earned by using certain hotspots, boosting adoption.

Integration with Public Services: Provide free or faster access to key government and social services via Wi-Fi. For instance, access to DigiLocker, e-learning portals, telemedicine, or farmers' market rates could be zero-rated or prioritized. Hotspots at schools could automatically give students homework-portal access without charge. This blends monetisation with public value – even if normal traffic is limited, enabling education/health content expands social welfare.

Local Business Sponsorships: Small businesses can sponsor a nearby hotspot. For example, a local kirana or pharmacy could cover the cost of a

hotspot at a community center in exchange for advertising on the login page. This crowdsources funding to the local level, and in dense markets can cover O&M costs through minimal ad revenue.

Transit/Ticket Bundles: Similar to airlines bundling in-flight Wi-Fi, Indian transit could do so. A train or bus ticket (physical or app-based) might come with a Wi-Fi voucher. This is effectively a sponsored model (the transport authority or a sponsor pays for the user's data).

State/School Wi-Fi Schemes: State governments could establish targeted Wi-Fi subsidy schemes. For example, a "Free Wi-Fi for Students" program could give schoolchildren a daily data quota at local hotspots. MSME clusters could similarly get supported Wi-Fi to enable e-commerce. Such schemes channel funds to hotspot providers on condition of free or discounted service to target groups.

Micropayment and Token Models: Emerging fintech like token rewards (users earn tokens for viewing ads or helping extend coverage) could be explored, especially among youth in urban slums or campuses.

Each of these should be piloted carefully, with guidelines to prevent misuse (e.g. ensuring free public sites remain open, no paid "sponsored Wi-Fi" traps).

4. Consumer Protection & Transparency

Any monetisation must respect consumer rights. Key safeguards include:

Free/Basic Access Guarantee: Mandate a free basic service tier everywhere (for example, a certain data/time per day at ~1–2 Mbps). This

preserves digital inclusion. Paid models should be optional add-ons, not gatekeepers.

No Predatory Upselling: Hotspot providers must clearly disclose charges and not obligate users into high costs. Plans and pricing must be shown transparently before login, not buried in fine print. Sale of paid upgrades should be voluntary and with clear cancellation options.

Data Privacy and Non-Discrimination: Wi-Fi login should not require downloading arbitrary apps or sharing data beyond simple KYC. User data (browsing habits, locations) must not be sold without consent; analytics should be aggregated and anonymized. Access providers should not discriminate or throttle certain content/services.

Quality-of-Service (QoS) Benchmarks: Even free tiers should meet minimum speed and uptime standards. TRAI could set QoS standards (e.g. ≥1 Mbps for basic tier, ≥5 Mbps for premium tier) and performance metrics. Disbursements or subsidies should be contingent on meeting QoS and usage targets (e.g. uptime >99%, certain GB/month usage) to avoid ghost projects.

Grievance Redressal: Hotspot providers must provide a quick complaint mechanism (toll-free number or app) for issues like downtime or overcharging. ULBs or TRAI should monitor compliance periodically.

These protections ensure monetisation does not come at the cost of digital rights and trust. Experience shows that overly restrictive or opaque pay-walls repel users; transparent, fair practices encourage broader adoption of Wi-Fi services.

5. Technology-Neutral, Future-Ready Perspective

The above models should be technologically agnostic and accommodate future networks:

5G/6G Offload: Public Wi-Fi can offload traffic from congested cellular 5G networks. Carriers should be encouraged to let their subscribers use Wi-Fi hotspots freely (via Passpoint/Hotspot 2.0 roaming). Future 6G will likely integrate Wi-Fi protocols; densifying Wi-Fi hotspots (urban fiber-fed or mmWave) complements 6G's small-cell visions. Thus, Wi-Fi expansion directly supports mobile network quality.

Fiberisation and Neutral-Host Backhaul: Government must continue funding fiber to towers/POPs. A dense fiber backbone (BharatNet, city fiber rings) is the anchor for all hotspots. Additionally, promote neutral-host data centers or edge nodes where multiple operators interconnect. Shared fiber ducts and poles reduce capex.

Edge Caching and CDN Integration: Hotspots in high-usage zones (cities, campuses) should incorporate edge caching (store popular videos, updates). This improves user experience and reduces backhaul cost. PM-WANI architecture could allow CDNs to cache content at hotspot level.

Satellite and Wireless Backhaul: As low-cost LEO satellite internet becomes available, encourage a hybrid model: remote hotspots use satellite for last-mile, with dynamic switching to 4G/5G where available. Satellite providers could partner with hotspot aggregators to offer subsidised data in hard-to-reach areas, ensuring even the most remote schools can have Wi-Fi.

Neutral-Host Networks: For example, cities can build shared wireless infrastructure (on lampposts or bus stops) usable by any ISP. This avoids split incentives where one operator builds only where profitable. Smart cities can adopt such models to achieve universal coverage.

These approaches keep the framework adaptable. In all cases, regulatory neutrality is key: the policy should not favor any single technology or operator but support any that meets coverage and cost goals.

6. Differentiated Strategy & Recommendations

A balanced, differentiated monetisation approach will best serve India's public Wi-Fi goals:

Rural: Focus on public support and community models. Government (USOF/BharatNet) must provide backhaul and initial subsidies (VGF) so that rural hotspots can offer a free basic tier. Encourage NGOs/CSR to run social hotspots at schools, health centers, markets. Foster micro-entrepreneurs (shops, gram panchayat kiosks) with equipment grants. Even if user revenue is minimal, the benefits (literacy, e-governance) justify ongoing funding.

Urban: Deploy mixed models. Use freemium and ad-supported Wi-Fi broadly (parks, markets, slums) to cover diverse income groups. Stimulate PPP projects for harder-to-serve neighbourhoods via municipal funding. Incentivize carriers and venue owners to bundle or share revenue. For instance, a smart city might install Wi-Fi in public Wi-Fi in underserved zones (subsidizing 50% capex), leaving 50% to an operator who then shares ads revenue. This keeps urban roll-out vibrant without full subsidies.

High-Footfall: Lean on commercial and sponsorship models. Airports, railway stations, stadiums, tourist spots should mostly be self-sustaining.

Ensure paid plans, premium QoS tiers and data-sale opportunities are available. Engage advertisers and venue owners in revenue-sharing deals. Even here, mandate a modest free tier for needy users, but allow the bulk of capacity to be monetised. These locations generate enough ARPU to justify investments, so they should not rely on subsidies except perhaps on capital re-use (e.g. reusing ducts).

Across all geographies, the core principle is sustainability with inclusion: monetisation must not lock out any user from a minimum connectivity level. Public funding or partnership should plug gaps, especially for rural and low-income urban pockets, whereas market-driven models can flourish in denser, more affluent settings.

Consumer Focus: All models must center on user benefit. Affordable or free access for students, gig workers, MSMEs and the poor expands economic opportunity. Higher-tier plans should enhance, not restrict, user choice. Quality must not be sacrificed to cut costs. Transparent pricing and privacy safeguards will build trust (for example, the first 1–2 Mbps being truly usable encourages wider adoption).

Sustainability: By aligning incentives (e.g. venues earn ad revenue, ISPs offload traffic, governments achieve inclusion targets), we create a virtuous cycle. A well-monetised Wi-Fi network relieves pressure on mobile networks and stimulates data-driven local economies – these broad gains justify initial support. Neutral-host and fiber-first backhaul ensure that networks remain efficient.

International Lessons: We have drawn on global examples: EU broadband funding often prioritizes fiber to underserved areas first; Singapore's Wireless@SG uses a shared-infrastructure approach; Brazil and Indonesia

run subsidized village connectivity programs. A hybrid strategy combining grants, PPPs, CSR, and user-pay models (as TRAI's consultation suggests) is thus prudent.

In summary, no single model fits all. A mosaic of monetisation methods – free basic service with government/community support in rural zones, mixed ad/premium models in cities, and commercial sponsorship in busy hubs – will together sustain India's public Wi-Fi growth. This differentiated, technology-neutral framework will maximize coverage and reliability, keep services affordable, and maintain open access, ultimately driving digital inclusion without compromising financial viability.

Q26. Please provide any additional comments, observations, or suggestions related to the proliferation of Public Wi-Fi in the country, including any potential issues or considerations that may not have been covered in the sections above. Please provide your response in detail with justification.

Comments :

Systemic Gaps in Public Wi-Fi Deployment

Public Wi-Fi networks in India face several infrastructure and policy gaps that limit their effectiveness. Backhaul availability and redundancy: Urban and rural Wi-Fi alike depend on reliable high-capacity backhaul. While India has vastly expanded middle-mile fibre (e.g. BharatNet's 7.22 lakh km of fibre connecting over 218,000 Gram Panchayats), last-mile fibre to actual hotspot locations remains weak. As TRAI notes, "limited last-mile fibre extension to neighbourhoods, public locations and community spaces continues to

constrain…Public Wi-Fi hotspots". In practice this means a hotspot without nearby fibre can never deliver reliable bandwidth. Without redundant paths, even fibre-fed hotspots become unusable if that single link fails. In remote areas, terrestrial fibre may never arrive – here alternative backhaul (microwave or satellite) should complement fibre. Power and reliability: Many rural towns have frequent power cuts. Public Wi-Fi access points (hotspots) need continuous power just like mobile towers. Without backup batteries or solar support, hotspots will go offline during outages. Yet there is no uniform rule requiring backup for PM-WANI PDOs (Public Data Offices). As with telecom towers, backup generators or renewable backup should be mandated for standalone hotspots.

Device affordability and digital literacy: A nationwide Wi-Fi network cannot be used if people lack devices or skills. India's internet penetration is ~72% overall, but only ~47% in rural areas. Many low-income users cannot afford smartphones or data-capable devices; even when they can, they may not know how to connect to Wi-Fi. This gap suppresses demand. As one analysis urges, "Device affordability is also key: schemes for low-cost data-capable phones and digital literacy camps can boost demand and inclusion". Without tackling device cost and user skills, public Wi-Fi will remain underused in villages and slums.

Security, privacy and data protection gaps: Public Wi-Fi by nature exposes users to risks. Data on open Wi-Fi can be intercepted by any nearby device. Experts observe that "the broadcast nature of Wi-Fi means that anyone within range of the network can receive and potentially read transmissions intended for any other device". Rogue hotspots can mimic legitimate ones (an "Evil Twin" attack) and harvest user credentials. Moreover, many users

do not appreciate these risks and connect casually. In the absence of strong security standards, user data (including location, browsing and personal details entered during login) can be collected or misused without clear consent. India's nascent data protection laws (DPDP Act) do not yet explicitly cover such edge networks. The PM-WANI framework should therefore include stringent privacy requirements: minimal data collection, encrypted authentication, and explicit user consent.

Fragmented local policies and accountability: Deployment is also stalled by inconsistent municipal rules and unclear agency roles. Although the Telecom RoW Rules 2024 have dramatically cut approval times (from ~455 days to ~30 days nationally), implementation is uneven. Some cities still levy extra fees or impose ad hoc conditions. In many cases, it is not clear whether State departments or Urban Local Bodies (ULBs) should lead a hotspot project. TRAI notes that "coordinated Centre–State–Local Body action is central" to scaling public Wi-Fi. Without clear governance—defining who installs backhaul, who funds hotspots, and who operates maintenance—projects can stall or overlap.

Consumer Protection Risks

Consumer interests must drive any public Wi-Fi plan. Several protections are currently weak or absent:

Privacy and Data Use: Public hotspots often require user registration (e.g. via mobile number or Aadhaar) and may gather personal data. Without clear rules, this data can be used for profiling or advertising. For example, third parties might aggregate log-in data to track footfall or marketing behavior. In

the Wi-Fi consultation, submissions warned that information like age, PIN code or browsing history is often collected and shared by sites without encryption. Consumer law must ban undisclosed data monetization and require granular consent for any data collection.

Transparent Pricing and Non-Discrimination: Even "free" Wi-Fi can entail hidden costs. Users should see clear terms: if service will slow after a cap, or if any content is blocked, it must be disclosed up front. Predatory practices – for instance upselling data packs mid-session or throttling common services – should be barred. Data services regulations in India already prohibit discriminatory tariffs; similarly, public Wi-Fi tariffs (even for paid tiers) must be plain, published, and non-discriminatory (no higher prices for streaming vs browsing, for instance).

Quality of Service (QoS): Wi-Fi networks can easily become congested, yielding very poor speeds or frequent disconnects. Consumers must not bear chronic outages or unusable service. TRAI's own analysis found coverage and speed complaints are the top consumer grievances. We recommend setting minimum QoS standards for public hotspots (e.g. 512 Kbps minimum throughput, 95% uptime) and linking subsidies or approvals to performance. Crowdsourced tools (like TRAI's MySpeed) should be extended to measure public Wi-Fi health.

Grievance Redress: Today, a user who feels cheated by a PM-WANI hotspot has no easy redressal path. There is no unified portal to lodge complaints about a PDO or PDOA. A national helpdesk (perhaps via the existing 7738 MyCall network) should be created for Wi-Fi grievances, with clear SLAs for resolution.

Accessibility and Inclusion: Special attention is needed to ensure equitable access. Portals should be easy to navigate for the elderly or differently-abled (e.g. multi-lingual login, screen readers). Women and girls may face privacy concerns using public Wi-Fi, so anonymity and safety (e.g. at community kiosks) is important. Outlets should be sited near schools, PHCs and women's self-help centers, with outreach so vulnerable groups actually benefit.

Recommendations to Strengthen PM-WANI and Public Wi-Fi

To address these gaps, we offer the following forward-looking measures:

National PM-WANI Dashboard: Create a transparency portal showing all registered PDOs/PDOAs and live hotspot locations. This enables users to find service, and lets regulators monitor network growth and performance. The dashboard could publish usage statistics, downtime reports, and key metrics for each hotspot, fostering accountability.

Unified Municipal Wi-Fi Policy: The Centre (MeitY/MoHUA) should issue model guidelines for city-level Wi-Fi deployment. These would standardize processes (RoW, fees, and street-furniture use) so that every ULB follows a single framework. For example, ease of access can be codified by allowing utility poles and bus shelters to host APs without extra charges. Several Indian cities (Mumbai's "Wi-Fi through street-light poles" initiative, for instance) have done this in ad hoc ways, but a national template would remove red tape.

Leverage Public Infrastructure: Ensure synergy with existing digital networks. All BharatNet/DBN Points of Presence should be opened to PM-WANI operators for backhaul. Likewise, RailTel's fiber at railway stations

and airports should be allocated for hotspots in transit areas. Government Common Service Centres (CSCs) and libraries – which often lie on BharatNet – can host Wi-Fi APs. In short, treat BharatNet/SmartCity/CSCs as the "middle-mile" for public Wi-Fi.

Targeted Community Programs: Reserve funding (from USOF or CSR) for hotspot projects in priority locations. For example, allocate subsidies or grants specifically to set up Wi-Fi at 1) schools, 2) health clinics, 3) panchayat offices, 4) women's training centers, 5) MSME clusters. Encourage models where Village Panchayats or cooperatives run a hotspot (as PDO/PDOA) as a social enterprise. State governments can act as PDOAs in villages (as TRAI suggests) or join with private partners via PPP. Kerala's Eraviperoor Gram Panchayat free Wi-Fi is an inspiring case. Priority should go to economically vulnerable or remote communities where private investment is hard to attract.

Entrepreneurship and Inclusion Incentives: Provide special incentives for local entrepreneurs to set up as PDOs, especially women, SC/ST or disabled entrepreneurs. For instance, seed grants or interest-free loans could be given for startup costs, along with free training. A quota (say 10–20%) of PM-WANI funding earmarked for social enterprises would ensure the network is citizen-owned, not just run by large ISPs. Consumer groups have noted that empowering village technicians and women entrepreneurs not only creates jobs, but makes network maintenance more sustainable locally.

Emergency and Social Uses: Mandate that every new hotspot have a backup battery for at least a few hours of power outage, so it can serve as a communication node during disasters. In cyclone/flood zones, Wi-Fi units

can even be pre-positioned with solar panels. Encourage local authorities to use PM-WANI for public alerts (e.g. sending emergency messages via Wi-Fi in a market area). Similarly, integrate Wi-Fi with social services: for example, schools could give free Wi-Fi to students for e-learning in the evenings, or health centers could offer patients online telemedicine via nearby hotspots. Linking public Wi-Fi to DigiLocker portals or e-governance kiosks at Panchayats can also expand digital services.

Technology-Neutral and Future-Ready Innovations

The public Wi-Fi ecosystem should embrace open standards and emerging tech:

Cellular Offload: As 5G and future 6G rollouts expand, policy should explicitly support offloading traffic to Wi-Fi. TRAI notes that offloading to Wi-Fi can reduce network congestion and improve QoS. Operators should be encouraged (via spectrum roll-out conditions or incentives) to offer integrated Wi-Fi offload for hotspots in dense areas or campuses, freeing up cellular spectrum for coverage.

Neutral-Host Models: In high-footfall venues (malls, stadiums, universities), multiple carriers should share a common Wi-Fi infrastructure. This neutral-host model (similar to in-building DAS) avoids duplicate cabling and allows any authenticated user to access the same network. Countries like Singapore and the US have seen success with shared Wi-Fi networks backed by standards (e.g. Passpoint). Our telecom policy should facilitate neutral-host deployments by allowing third-party providers to build and lease Wi-Fi networks to all service providers.

Satellite and Hybrid Backhaul: For truly remote or dispersed communities (e.g. island villages, border outposts), satellite backhaul is now affordable. Rather than wait for fibre, hotspots can use modern LEO or GEO satellite links as primary backhaul. Similarly, Local Multipoint Distribution Service (LMDS) or TV white space can be used. Policy should allow government or PDOAs to use these technologies (including subsidizing the equipment) to "skip" fibre where it is uneconomic. This ties into India's growing space-based digital infrastructure (Nusantara satellites) and can connect hard-to-reach hamlets under one Wi-Fi umbrella.

Edge Caching and Local Content: In busy zones, popular content (educational videos, govt apps, local news) can be cached on on-site servers or edge nodes to reduce backhaul load. Public–private partnerships can establish small caching servers at hotspots (as done in some global "community Wi-Fi" pilots) so that repeated requests don't all travel over expensive links. This improves user experience and cuts data costs – particularly important where backhaul is slow or metered.

Open Standards and APIs: Adopt and promote seamless authentication standards (e.g. Hotspot 2.0/Passpoint) so that users don't need to enter credentials at each location. A robust Wi-Fi also requires an open interface for payment and roaming – for instance, integrating PM-WANI hotspots with the Unified Payments Interface (UPI) or mobile wallets, as suggested in earlier TRAI proposals. Further, open APIs should allow apps and devices to discover and connect to trusted Wi-Fi (while protecting privacy), following models like the Wireless Broadband Alliance's OpenRoaming. Such

technology-neutral approaches ensure future networks (Wi-Fi 6E/7, private 5G, etc.) can interoperate smoothly.

Governance and Regulatory Measures

Strong oversight and consumer safeguards will ensure the network's integrity:

Certification and Quality Standards: The government should establish a certification regime for PDOs and PDOAs. Any entity deploying a hotspot (especially with public funds) must meet minimum quality and security requirements. For example, mandatory encryption on all Wi-Fi radios (to prevent snooping), periodic security audits, and DSCI-like auditing for data protection. Models like ISO/IEC 27001 could be adapted for PDOs.

Performance Audits: All funded hotspots (state-subsidized, PPP, or CSR) should report usage and performance metrics to an independent body. Periodic audits (by TRAI or an empowered agency) can verify uptime, speed, and consumer complaints. Funds can be released in tranches based on hitting milestones – for example, actual user-hours or minimum speed delivered. This ensures accountability for public money.

Data Privacy by Design: Regulations should mandate that PM-WANI authentication and login processes collect no more data than necessary. By default, logs should be anonymized or encrypted. Operators/PDOs must follow the Personal Data Protection Act's principles (consent, purpose limitation, data minimization) even before it fully comes into force. Any marketing or analytics must be opt-in. Clear privacy notices (in local languages) should be required at login portals.

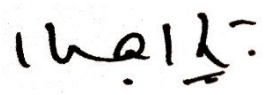
Defined Roles and Collaboration: Clarity of roles is critical. The Centre should remain the policy anchor and funding source for national backhaul (BharatNet, Satellite mission) and regulatory standards. State governments can coordinate rural deployments and even act as PDOAs for remote panchayats. Urban Local Bodies must be empowered (by law) to streamline RoW, provide street infrastructure (lampposts, kiosks) and maintain municipal networks. TRAI has underscored that "Central and State Governments, along with municipal bodies, [must] collaborate as facilitators" to accelerate roll-out. Formal inter-governmental task forces or a PM-WANI cell in each state could operationalize this coordination.

Conclusion and Vision

Public Wi-Fi must be a pillar of India's Digital Inclusion strategy – not a fringe project. By filling coverage gaps and lowering connectivity costs, a vibrant public Wi-Fi ecosystem will underpin goals in education, health, commerce and governance. Crucially, it must be affordable and trustworthy: users should know that hotspots are safe, reliable and non-exploitative. We envision a whole-of-government initiative where broadband deployment, digital literacy, and consumer protection are integrated from the start. The Wi-Fi network of tomorrow should be sustainable (using green energy and shared infrastructure), open (supporting neutral hosts and seamless connectivity), and user-centric. In short, India's public Wi-Fi rollout must mirror the success of its Aadhar and UPI projects by emphasizing universal access, data privacy, and ease of use. By learning from international examples (the EU's WiFi4EU grants, Singapore's nationwide Wireless@SG, Brazil's Wi-Fi Brasil schools program, Indonesia's village networks) and by tailoring those lessons locally, India can ensure that no citizen is left offline.

Public Wi-Fi, done right, will be a powerful enabler of Digital India: affordable, ubiquitous broadband that every student, entrepreneur, and worker can tap into with confidence.

Thanks.



(Dr.Kashyapnath)
President