TRAI Consultation 07/2026 — Response by R-Fi / INA Technologies Private Limited

Proliferation of Public Wi-Fi Networks in India | R-Fi / INA Technologies Private Limited

Founder: Rakesh Korumilli

Email: rakesh.korumilli@gmail.com

Filing deadline: 25-May-2026

To: advbbpa@trai.gov.in

CC: jtadvbbpa-1@trai.gov.in

Jump to section:

> ***Note on preparation:*** *This response was prepared using AI — technologies available today that enable a single founder, managing multiple professional and personal commitments, to engage substantively with a consultation of this scope. The document has been through multiple rounds of review and correction before submission.*

Preamble

INA Technologies Private Limited (CIN: U61900TS2026PTC216586, incorporated 20-May-2026 under the Companies Act 2013; Registered Office: 70 Gruhalaxmi Colony, Aoc Records, Tirumalagiri, Hyderabad,

Telangana – 500015) is the operating entity for R-Fi, a public Wi-Fi platform being built in Telangana. PDOA registration is planned under this CIN.

We write as practitioners, not theorists. Our predecessor network — OurFi, operated under INA Technology Solutions LLP — ran live hotspots in Hyderabad from 2016–2018 using MikroTik routers, a Hotspot Express RADIUS backend, and a proprietary captive portal with an offers and marketplace layer. We have independently verifiable operational records: 177 registered users confirmed in the Hotspot Express RADIUS report (October 2017), 190 unique users in our own application log (January–December 2017), PayU-processed payments at Rs.15/GB, and real session and failure data that directly inform our responses below.

Before we answer the specific questions, we would like to provide operational context — the practitioner's view from a team that has built and operated this model, in this market, under conditions harder than those that now exist.

Part 1 — The Awareness Case

> **Core argument:** The PM-WANI ecosystem is sound. The regulatory framework exists. The technology works. What remains is to unlock the synergies that are already latent within it — between venue owners, users, data buyers, advertisers, and government — and to do this systematically, at scale, under the right policy conditions. R-Fi's position in this consultation is to share, as a practitioner who built and operated this model before the current framework existed, the specific policy steps that would allow these synergies to become self-sustaining. TRAI's consultation paper (paras 2.140–2.142) identifies anonymised data monetisation as a

> potential PM-WANI revenue stream. PM-WANI is currently a connectivity framework — it does not address data monetisation. The DPDP Act 2023 governs consent and data processing but offers no PM-WANI-specific guidance. These two frameworks need to be explicitly connected — through a joint TRAI-MeitY effort that sets clear standards, and communicates them to every ecosystem participant: PDOAs, device owners, data buyers, and users. Clarity, standardisation, and communication are what unlock the synergies already latent in this ecosystem. R-Fi would like to contribute towards shaping that framework — not as a commentator, but as a builder.

1. The Awareness Gap — The Central Problem

The consultation paper identifies the problem precisely. Para 2.93 states: *"Many potential users are not adequately informed about the availability of Wi-Fi hotspots, the access method, or the cost and reliability of such services."* It goes further: *"A perceptible lack of awareness persists among potential and existing PDOs. Many are not adequately informed that becoming a PDO involves minimal entry barriers, with no licensing requirement and only a simple registration process."* We do believe that this is one of the key barriers to hotspot proliferation, yes. It is TRAI naming, in its own words, the central barrier to PM-WANI proliferation.

The paper's formal questions lead with supply-side constraints, backhaul, funding, and authentication. The practitioner's argument — which R-Fi is uniquely positioned to make — is that all of those interventions will underperform as long as the awareness gap goes unaddressed. Infrastructure without awareness is infrastructure that sits idle.

India's own deployment gap makes the case. The National Digital Communications Policy 2018 targeted 10 million public Wi-Fi hotspots by 2022. As of April 2026 — four years past that deadline — PM-WANI has 4,10,131 hotspots: approximately 4% of the target. This is not an infrastructure failure alone. The paper acknowledges (para 2.87) that *"the widespread expectation of free Wi-Fi acts as a significant psychological and economic barrier"* and (para 2.88) that users find

mobile data more convenient even when public Wi-Fi is available and cheaper. These are awareness and perception problems, not access problems.

Three awareness gaps operate simultaneously — and each requires a different intervention:

- **Customer awareness:** Users see public Wi-Fi as a free utility — identical to the Hy-Fi at the metro station. They do not know that a well-designed PDOA platform delivers hyperlocal offers, venue promotions, and relevant services at the moment of connection. The value exchange is invisible. Para 2.90 confirms: *"users often prefer the perceived safety of their mobile data networks"* — not because public Wi-Fi is unsafe, but because no one has clearly communicated what it is, what it protects, and what it gives them.
- **Device owner awareness:** Hotspot operators — kirana stores, cafes, training centres — see themselves as providing a service, not sitting on an asset. They do not know they hold an advertising surface, a footfall data layer, and a direct marketing channel to their own customers. This is why PDOA economics fail at the small operator level: the revenue streams exist but the venue owner has no visibility into them. Our version 1 experience confirmed this directly — venue owners were surprised by the revenue potential once it was demonstrated.
- **Policy awareness:** The consultation paper discusses data monetisation (para 2.142) without once mentioning the DPDP Act 2023 — the legislation that governs exactly how that monetisation must be designed. In 109 pages, India's own data protection law is absent from India's own public Wi-Fi consultation. This is the policy awareness gap: the integrated model of connectivity + consent + data value has not yet been named as a coherent government objective. We are naming it here and contributing to making this clearer.

The depth of this awareness gap deserves to be stated plainly. Public WiFi is not a utility in the way electricity is a utility. It is a proximity commerce and communication platform — the nearest point between a consumer and the venue they are physically standing in. Think of air as the communication medium: present everywhere in that space, connecting everything within it. The platform is the seamless connective tissue that makes that medium useful and commercially

valuable. With minimal data shared — within the complete protection of privacy law and user consent — it enables targeted local offers, neighbourhood commerce, and contextual services at the exact moment of need. The user who connects does not just receive data. They receive relevant offers from the venue, promotions from nearby businesses, and access to a commerce layer anchored to their physical location. This is the dimension of value that the awareness gap conceals — not just from users, but from venue owners, regulators, and policymakers alike. Our version 1 experience confirmed it directly: venue owners who saw their first additional revenue through the offers layer responded with genuine enthusiasm. The commercial case was not theoretical to them — it was immediate. The regulation should enable and protect this awareness shift.

From the TRAI consultation paper (CP 07/2026) — extracted 21-May-2026:

- **Deployment gap:** NDCP 2018 target = 10 million hotspots by 2022. PM-WANI reality = 4,10,131 hotspots (April 2026). 96% short, 4 years late.
- **TRAI names the awareness gap directly (para 2.93):** "Many potential users are not adequately informed about the availability of Wi-Fi hotspots, the access method, or the cost and reliability of such services." Also: PDOs are unaware of minimal entry barriers and income potential.
- **Free WiFi expectation (para 2.87):** "The widespread expectation of free Wi-Fi acts as a significant psychological and economic barrier to the expansion of Public Wi-Fi, as it directly weakens the commercial viability of hotspot providers."
- **Security/trust barrier (para 2.90):** "Security, privacy, and trust deficits pose a significant barrier to the widespread adoption of Public Wi-Fi networks." Users cautious about "open networks managed by small entities such as local shopkeepers."
- **Data monetisation endorsed (para 2.142):** "Aggregated and anonymised usage and footfall data can be monetised by venue owners, urban authorities, and planners." Named as a legitimate indirect revenue stream — but DPDP Act 2023 not mentioned once in the paper.
- **Smart Cities gap:** Only 39 of 100 Smart Cities Mission cities have launched public Wi-Fi — despite all having deployed CCTV and fibre infrastructure. Same backbone, no Wi-Fi layer.

- **US comparison (para 2.24 — cited by TRAI):** 43% of US residents consider public Wi-Fi essential infrastructure for daily connectivity. 39% concerned about privacy. India's lower demand is attributed to cheap mobile data — not absence of demand.
- **India mobile data pricing (Annexure I):** Jio Rs.5.69/GB, Airtel Rs.10.67/GB, average Rs.8.18/GB. PM-WANI best plan: Rs.0.99/GB (monthly). Cost is not the barrier. Awareness and trust are.

R-Fi's own primary research — a demand survey of approximately 79 users in Hyderabad conducted in December 2025 — provides ground-level data that complements and sharpens the TRAI paper's analysis. The respondents were predominantly 15–30 year old prepaid mobile users (approximately 90% prepaid), engineering college students, and high data consumers (over 80% using more than 1 GB per day). This is precisely the target segment for PM-WANI expansion.

The survey's most important finding is that the awareness gap is exactly as real as the consultation paper describes — but its shape is more specific. Over 70% of respondents said they are always actively looking for Wi-Fi access. This is not passive awareness — it is unmet demand. Users want Wi-Fi but have not found a platform they can trust. When asked for their primary reasons not to use a public Wi-Fi platform, security concern was the leading response. And yet over 40% of respondents said they are comfortable and see no reason not to use it at all, even when explicitly asked to find one. The security barrier is real — but it is winnable. It is a trust deficit, not a deep structural objection. The implication for policy is direct: users with confirmed demand are being held back not by lack of awareness of Wi-Fi as a concept, but by absence of a visible, government-backed trust signal that a specific platform is safe.

From R-Fi primary demand survey (Dec 2025, ~79 respondents, Hyderabad):

- **Active demand confirmed:** Over 70% of respondents are always looking for Wi-Fi. 90% are on prepaid mobile plans — the cost-sensitive segment most likely to benefit from a Rs.15/GB alternative.

- **High data consumption:** Over 80% use more than 1 GB of mobile data per day. These are exactly the users for whom a cheaper Wi-Fi option delivers meaningful monthly savings.
- **Price point validated:** Rs.15/GB sits exactly in the preferred price range (Rs.5–30 per GB). Survey confirms this was and remains the right pricing. TRAI's Annexure I shows average mobile data cost is Rs.8.18/GB — Wi-Fi at Rs.15/GB is not cheaper per GB, but the higher speed, venue anchoring, and data plan structure create a distinct value proposition.
- **Core demand signal — speed, cost, plan validity:** The survey is unambiguous on what users want. Speed is the single most important factor in a secure WiFi connection — 68% rated it Most Important or Very Important. Cost savings is the #1 reason users would choose OurFi — 60% named it as their top reason. Plan validity ranks third (35% Most or Very Important) — users want access that lasts, not connections that expire mid-use. R-Fi's model directly addresses all three.
- **Security trust = primary barrier:** Security concern was the leading stated reason not to use a public Wi-Fi platform. Combined with the TRAI paper's para 2.90 finding ("users often prefer the perceived safety of their mobile data networks"), this is a consistent cross-source signal. The fix is not more advertising — it is a visible trust marker. A certification standard — analogous to BIS marking on electronics — showing that a platform is DPDP-compliant and data-safe would directly address this barrier.
- **40%+ already comfortable:** Over 40% of respondents said they see no reason not to use a public Wi-Fi platform. The security-concerned segment is real but not dominant. This market is already partially ready.
- **Supply side: mixed hosting intent, but idle broadband capacity is real:** When asked directly about their preferred role in the platform, approximately 37% clearly chose hosting a hotspot. Over 50% of existing broadband subscribers do not exhaust their FUP data limit monthly — idle capacity that could serve as supply. The hosting intent signal is real but should not be overstated: the supply constraint is partly willingness, but primarily the absence of a trusted, certified platform through which to host.
- **Offers and marketplace: invisible but valued:** Users are largely unaware of the hyperlocal offers and marketplace layer — only 1 in 63 respondents (1.6%) chose personalised offers as their primary reason to use OurFi, yet version 1 OurFi marketplace saw real traction once users were exposed to it. The depth-of-value

awareness gap (knowing Wi-Fi exists vs knowing what connecting actually unlocks) is the next layer TRAI's awareness interventions should address.

- **UPI = dominant payment preference:** Clear majority preference in survey. Consistent with TRAI's own authentication recommendations. A UPI-based Wi-Fi payment model removes friction and leverages existing user familiarity.
- **Location preferences:** Gym and restaurant are the highest-priority locations for users. College settings show ambivalence — high interest AND high security concern among the same student cohort, confirming that the security barrier is most acute in high-density peer environments where reputational risk is felt most.
- **50% want to continue in the project:** Retained interest after the survey. Warm leads for pilot deployment.

2. The Synergy Map — What Most Stakeholders Cannot See

The R-Fi model is not a hotspot business. It is a platform that sits at the intersection of five stakeholder needs — and creates value for all of them simultaneously. This is the synergy that needs to be made visible to TRAI.

The following describes the R-Fi platform model — validated through version 1 operations (2016–2018) and being rebuilt under INA Technologies Private Limited.

Stakeholder	What they need	What R-Fi delivers
Wi-Fi User	Affordable connectivity, security assurance, relevant offers	Free / low-cost access + consent-gated personalised offers + DPDP-protected data

Device Owner (hotspot operator)	Income from the hotspot, easy management, customer visibility	Hosting revenue from idle broadband capacity + captive portal as a zero-cost proximity marketing surface (virtual billboard) + offers layer to promote their own products and services to every connected user at the point of physical presence
Local Business and Advertisers	Reach to nearby or targeted customers at the right moment — whether a kirana store at the same location or a national brand targeting a specific demographic cohort	Hyperlocal offer placement on captive portal and post-login in-app; programmatic reach to verified location-anchored audiences at scale
Data Buyer (fintech, FMCG, real estate, quick commerce)	Footfall data, behavioural cohorts, location analytics	Tier 1 anonymised aggregated data — DPDP-compliant, commercially actionable
Government / TRAI	PM-WANI proliferation, digital inclusion, sustainable PDOA economics	Self-sustaining PDOA model at scale — data and ad revenue as the engine for long-term viability

No single policy lever, no single infrastructure investment, and no single revenue model achieves all five simultaneously. The platform model does. This is the synergy argument — and it needs to be made explicitly in the TRAI response, not left for the reader to infer.

The most vivid illustration of this multi-sided value creation came from version 1 operations. A hostel owner in Hyderabad was spending approximately Rs.2,000 per month on a broadband connection — a pure operating cost with no return. After joining the OurFi network as a device owner, the same broadband connection began generating approximately Rs.200 per month in net hosting revenue, while

also serving the hostel's own guests. The net shift was not Rs.200 gained — it was Rs.2,200 recovered: a cost centre converted into a revenue line. The broadband bill that was leaving the business every month was now more than covered by the platform. The hostel owner did not change their infrastructure. They changed their relationship to it.

This is the synergy in practice. A single connection event — one user logging in at the hostel — simultaneously delivered affordable data to the user, generated hosting revenue for the venue, created an advertising surface on the captive portal, and added a data point to the anonymised footfall layer. No single stakeholder engineered this outcome. The platform produced it as a natural byproduct of the model. This is precisely what TRAI's awareness interventions should be communicating to potential device owners across India — not just that they can register as a PDO, but that their existing broadband connection is an asset they are currently giving away for free.

(Note: Hostel case study based on first-person founder experience from version 1 operations, 2017. Figures are indicative, not independently verified.)

3. The Green Argument — PM-WANI as a Circular Economy Initiative

The environmental dimension of public Wi-Fi proliferation is underrepresented in the consultation paper. The R-Fi model — and the PM-WANI framework more broadly — is one of the most environmentally efficient ways to deliver broadband-equivalent access in urban and semi-urban India. TRAI should recognise and actively position this.

Green IT and the circular economy. The European Union has required ISPs and telecom operators to implement circular economy models and meet binding energy efficiency and eco-design standards for network equipment. This is now a global direction of travel for the sector. India has an opportunity to align its PM-WANI policy with this trajectory — not by mandating compliance, but by recognising that the PDOA model is already structurally circular. The R-Fi model runs on existing hardware deployed in existing venues. No new towers, no new

spectrum, no new excavation. The infrastructure investment is a router, a broadband subscription, and a configuration. This is the circular economy applied to connectivity infrastructure — and it deserves explicit recognition in India's public Wi-Fi policy.

- **No new towers.** PM-WANI hotspots use routers already present in homes, shops, hostels, and training centres. The marginal cost of adding a hotspot node to India's connectivity infrastructure is a fraction of any cell tower deployment.
- **No new spectrum.** Wi-Fi operates on unlicensed 2.4GHz and 5GHz bands. No spectrum auction, no tower rental, no right-of-way excavation required.
- **Lower power at every layer.** Wi-Fi networks transmit data over short distances using significantly less power than macro cellular towers. When a user switches from mobile data to a local Wi-Fi connection, energy consumption drops at both the network infrastructure level and the personal device level — a battery and a power grid benefit simultaneously. Modern Wi-Fi infrastructure relies on fibre optic backbones, which release far less CO_2 per gigabit of data than copper-based alternatives and can be powered by renewable energy with minimal conversion loss.
- **Community infrastructure model.** The hotspot is embedded in an existing venue. The venue's electricity, premises, and staff absorb the fixed cost. The marginal energy cost of serving additional users is minimal — the infrastructure is already on.
- **Lifecycle extension.** Millions of routers sit underutilised in Indian homes and small businesses. PM-WANI gives these devices a productive second life as shared infrastructure — the circular economy principle applied directly to consumer electronics.

IoT and smart infrastructure readiness. Public Wi-Fi networks are not only a connectivity layer — they are a foundation for IoT-enabled smart infrastructure. Wi-Fi-linked wireless sensors can track environmental data, manage automated smart lighting, and optimise renewable energy outputs from wind and solar installations. A distributed PM-WANI network, once at scale, becomes the

backbone for smart city applications that India's urban infrastructure currently lacks the last-mile connectivity to support.

India's case to lead. Community Wi-Fi models in apartments, schools, colleges, and public spaces already embody green digital infrastructure — connectivity built on what exists rather than on new construction. PM-WANI is a circular economy initiative whether or not it is labelled as one. Including this dimension in TRAI's final recommendations would cost nothing to add. PM-WANI is not just a connectivity initiative — it is India leading the global Green IT movement, building on community infrastructure rather than replacing it.

4. Security Concerns — Building Trust Through Clear Standards

The consultation paper (para 2.90) clearly shows that security and privacy concerns are a significant barrier to public Wi-Fi adoption. Users are not wrong to be cautious — the current regulatory landscape gives them no clear signal about what is and is not permitted.

The right response would be to resolve them with clarity:

- TRAI and MeitY should jointly publish a clear, plain-language statement of what a PM-WANI PDOA *can* and *cannot* do with user data — not buried in regulatory documents, but published as a user-facing standard.
- The DPDP Act 2023's consent framework, properly implemented, is a strong security foundation. But users will not trust it until they are clearly and actively informed that it applies to public Wi-Fi.
- A visible "DPDP Compliant" marker on PM-WANI certified hotspots — analogous to BIS certification on electronics — would give users immediate assurance without requiring them to read a privacy policy.

> **Survey evidence — cross-source:**
>
> - **TRAI paper para 2.90:** "Security, privacy, and trust deficits pose a significant barrier to the widespread adoption of Public Wi-Fi networks." Users are cautious about "open networks managed by small entities such as local shopkeepers."

> - **R-Fi primary survey (Dec 2025, ~79 respondents):** Security concern was the leading stated reason not to use a public Wi-Fi platform — cited by the majority of respondents who gave a reason for non-use.
> - **The barrier is winnable:** Over 40% of the same survey respondents said they are comfortable and see no reason not to use public WiFi at all. The security-concerned segment is real but not dominant — and it is directly addressable through clear government communication.

The right model already exists in India. The Reserve Bank of India has run sustained, mass-reach awareness campaigns on safe digital transactions — covering ATM safety, card security, UPI dos and don'ts, and phishing awareness. The Amitabh Bachchan and other associated public service communications successfully moved a generation of first-time digital users from fear to comfort to habit. The outcome was not just individual safety — it was the mass adoption of UPI as a national payments layer.

Public WiFi needs exactly the same intervention. The government can publish and actively promote a simple, plain-language set of 4–5 rules for public WiFi use — not a regulatory document, not a terms of service, but a public awareness message. For example:

- Do not conduct banking or financial transactions over public WiFi
- Check that websites you visit use HTTPS (look for the padlock icon)
- Verify the network name with the venue before connecting
- Prefer platforms that display a DPDP Compliant or PM-WANI certified marker
- Log out when done — do not leave sessions open on shared connections

Five rules. Follow them, and be worry-free. This is the message India's public WiFi awareness campaign can carry. It requires the same communication investment that made digital payments safe in the public imagination.

The same principle extends across every participant in the ecosystem, not just end users. A hotspot owner configuring a router for the first time needs to know about OTP handling, session timeout settings, captive portal compatibility, and consent disclosure requirements — not through trial and error, but from a published

operational reference. A data buyer approaching a PDOA needs to know what compliance looks like and what consent architecture the platform has implemented, before any commercial discussion begins. A BIS-style certification mark for PM-WANI PDOAs — backed by a published checklist of operational and compliance standards — would give all three stakeholder groups a common, visible reference point. Certification becomes a signal everyone can read: this platform has been built to standard.

The cost of operational knowledge gaps is borne by early users, not operators. A misconfigured OTP flow or an unexpected session timeout does not generate a bug report — it generates a user who stops using public WiFi and does not come back. Every confusion event is a silent attrition event. Version 1 experience illustrates this concretely: discovering that a delayed OTP resend with a fresh code outperforms an immediate resend of the original required real deployment experience. Once discovered, the fix took minutes. But the learning was borne by real users who encountered failed logins before the fix was in place. At ecosystem scale, this class of avoidable failure accumulates into measurable penetration drag. Government-published operational standards — and the awareness and training campaigns that communicate them to hotspot owners, users, and other stakeholders — are not administrative overhead. They are the mechanism that shifts the entire ecosystem from learning-by-doing to starting-from-confidence. Time spent navigating confusion becomes time spent using the network. This is the marketing and educational transformation the PM-WANI ecosystem needs.

A critical policy distinction: perception risk vs technical mandate. The security concern in our survey — and in TRAI's own paper — is a perception problem, not a technical architecture problem. Open WiFi with a captive portal is the global industry standard for public WiFi, used by every airport, hotel chain, and coffee brand worldwide. The login page is served over HTTP by technical necessity (HTTPS cannot be intercepted for redirection). Once authenticated, all user traffic — banking apps, social media, messaging — operates over HTTPS exactly as it would on mobile data. The platform is not inherently less secure than mobile data. What users lack is the visible signal that tells them this. The policy error would be to respond to a perception problem with a technical mandate —

requiring WPA3 Enterprise, 802.1X authentication, or other enterprise-grade standards at the PDOA registration level. These raise the infrastructure cost floor significantly, price out every small PDO, and concentrate the market among large operators — without meaningfully improving security for the typical public WiFi use case. The right instrument is a trust certification mark (DPDP Compliant, PM-WANI certified) that gives users an immediate visible signal, combined with the government awareness campaign described above. Technical mandates belong on a phased roadmap for reference — not as a launch prerequisite, as that might hurt adoption.

The parallel to online transactions is instructive. A decade ago, a significant share of Indian consumers refused to transact online — not because online banking was unsafe, but because no one had clearly told them how to use it safely. Government-backed awareness, simple rules, and visible trust markers (the padlock icon, the OTP flow, the bank's logo) moved that population from refusal to reliance. The same arc is available for public WiFi — and the government is the only actor with the reach and credibility to initiate it. TRAI should recommend this explicitly as a policy deliverable alongside the infrastructure and regulatory asks in this consultation.

Show real stories, not just rules. Educational campaigns work best when they are anchored in recognisable, real-life situations. TRAI and MeitY should commission and broadcast stories that demonstrate two things simultaneously: what public WiFi enabled, and how it was safe. Two categories of story are particularly powerful:

- **Business value stories:** A gym owner who ran a membership promotion through the captive portal and signed up twelve new members in a week. A restaurant that showcased its signature dishes and a limited-time drinks offer at the login screen — and saw orders increase during the evening rush. These are not hypothetical scenarios. They are the natural outcome of a well-designed PDOA marketplace layer, and they speak directly to the device owner audience that PM-WANI needs to recruit at scale.
- **Emergency connectivity stories:** A student at a railway station whose mobile data stopped working during a network outage, and who found

connectivity through a PM-WANI hotspot to reach their family. A small business owner who needed to send a time-sensitive document when cellular congestion made their phone unusable, and who relied on a neighbourhood hotspot to get it done. These moments — when the mobile network fails and a trusted local WiFi connection saves the day — are more persuasive than any policy document. They build emotional trust in a way that rules and certifications cannot.

The government runs Doordarshan, All India Radio, and digital media campaigns at national scale. The infrastructure to deliver this storytelling already exists. What is missing is the decision to treat public WiFi adoption as a national communication priority — in the same way digital payments were treated as one. This is a recommendation TRAI can help validate and make in its final report.

5. Government Push — Standardise, Simplify, and Unlock the Ecosystem

PM-WANI is a well-designed framework. The operating model — connectivity, commerce, and data value creation converging at the moment of connection — is proven, economically sound, and aligned with India's digital agenda. TRAI's consultation paper identifies anonymised data monetisation and hyperlocal commerce as potential PM-WANI revenue streams (paras 2.140–2.142). PM-WANI is currently a connectivity framework — it does not address data monetisation. The DPDP Act 2023 governs consent and data processing without PM-WANI-specific guidance. The opportunity this consultation presents is to explicitly connect the two — through a joint TRAI-MeitY effort that sets clear standards and communicates them to every ecosystem participant. The question is not whether the ecosystem works. The question is what government can do to standardise and simplify the operating environment so that the synergies already latent in PM-WANI convert into actual deployment, penetration, and value at scale.

- **Standardise revenue sharing between PDOAs and device owners.** The model is self-propagating when every participant earns. A kirana store

hosting a router earns a share of the advertising or data revenue the hotspot generates. A data buyer gets consent-gated, anonymised footfall data. A user gets connectivity and relevant offers. No subsidy required — the economics work when the framework is clear. Government can help establish transparent, standardised revenue-sharing norms that make this the default rather than a negotiated arrangement.

- **Name data monetisation and hyperlocal commerce as intended PM-WANI outcomes — and explicitly connect PM-WANI with the DPDP Act 2023.** TRAI's consultation paper identifies these as potential revenue streams (paras 2.140–2.142). The next step is a joint TRAI-MeitY communication that sets out in plain terms what PDOAs can build with confidence and what data buyers can expect. That clarity — once published and communicated to all ecosystem participants — signals that this is a defined, structured path, not a grey area. That signal is worth more than any subsidy.
- **Communicate the opportunity to every stakeholder group directly.** Device owners who do not know they can earn from their broadband connection will not host. Data buyers who do not know the supply exists will not buy. Startups who do not know what they can build under PM-WANI will not build. The barriers are not technical or financial — they are informational. Government can help establish targeted communication for each group and dismantle these barriers systematically.
- **Offers and promotions through the platform create a natural local commerce channel.** When a user connects at a café and receives a relevant offer from a nearby business, that is contextual value delivery — the kind of synergy the PM-WANI ecosystem was designed to enable. Recognising this explicitly in TRAI's final recommendations would reinforce the integrated model.

> PM-WANI is a connectivity framework. The DPDP Act governs consent and data processing. Neither, on its own, gives a PDOA the operating clarity it needs to build a data monetisation model with confidence. The opportunity is for government to connect the two explicitly — through a joint TRAI-MeitY framework, awareness campaigns, PDOA support programmes, and policy language that names data

> monetisation and hyperlocal commerce as desirable, intended PM-WANI outcomes. Clarity, standardisation, and communication are what the ecosystem needs.

The barriers standing between PM-WANI's potential and its current 4% deployment reality are not primarily technical or financial. They are barriers of policy ignorance and lack of clarity — device owners who do not know they can earn from their broadband connection, potential data buyers who do not know the supply exists, and startups who do not know the regulatory framework permits what they want to build. Government push means systematically dismantling each of these barriers.

Strong, targeted educational campaigns directed at each stakeholder group are the first step — not generic awareness, but specific communication: what a device owner can earn, what a data buyer can access, what a startup can build on PM-WANI infrastructure, and what the rules are. When these barriers fall, the information highway opens.

The downstream value of that opening is significant. Internet connectivity, when made accessible in the right way to the right stakeholders, creates synergies that no single policy intervention could manufacture. Consider two examples among many:

- **ONDC and the R-Fi marketplace:** A buyer browsing on ONDC sees a seller's offer displayed on the R-Fi captive portal at the moment of connection — hyperlocal, contextual, and delivered through a government-backed open commerce infrastructure. Two national platforms, one moment of value. This is not a hypothetical integration — it is a natural consequence of the PM-WANI and ONDC frameworks operating in the same digital ecosystem.
- **Digital India AI startups and FMCG data:** A startup building on the Digital India stack uses anonymised, consent-gated WiFi session data to understand real consumption trends — what people in a neighbourhood are buying, when, and how often. It advises an FMCG major on what to sell, where, and at what price point. The FMCG major pays for the insight. The startup grows. The PDOA that generated the data earns a share. The user who consented gets better offers. Every participant gains.

These are not edge cases. They are the natural output of a well-designed, government-backed information highway — one where connectivity, commerce, and data flow together under a clear regulatory framework. India built UPI and showed the world that a public digital infrastructure, properly designed and actively promoted, can become self-sustaining and globally admired. PM-WANI, with the right government push, has the same trajectory. The government does not need to fund this ecosystem indefinitely. It needs to open the highway, set the guardrails, and step back. The stakeholders — PDOAs, data buyers, advertisers, device owners, and users — will do the rest.

It is also important to recognise that AI, IoT, Green IT, operational efficiency, and customer value creation are not separate policy tracks — they are one ecosystem, and public WiFi infrastructure is the connective tissue between them. An IoT sensor network needs ubiquitous WiFi to transmit. A Green IT model needs distributed, low-power nodes to replace energy-intensive macro infrastructure. An AI model needs real-world, consent-gated data to learn from. A customer receives value when all three layers — connectivity, data intelligence, and commerce — converge at the moment of connection. R-Fi understood this convergence early — building a platform that sat at the intersection of all four before the regulatory and technical frameworks fully existed to support it. Now, with the PM-WANI framework in place, the DPDP Act providing the consent architecture, and India's Digital Public Infrastructure stack maturing, the conditions exist to realise this vision at national scale.

This is directly aligned with the Viksit Bharat 2047 vision articulated by the Prime Minister — a developed, self-reliant India where digital infrastructure is universal, where every citizen has access to the information economy, and where Indian innovation leads globally rather than follows. A thriving, self-sustaining PM-WANI ecosystem — where neighbourhood hotspots generate data value, power local commerce, and connect every community to the digital economy — is not a peripheral policy objective. It is a building block of that vision. TRAI has the opportunity to say so clearly in its final recommendations.

6. R-Fi — The Right Fit

This submission is not theoretical. It is not a policy recommendation from a consultant who has studied this sector from the outside. It is a practitioner's account from someone who chose to build in this space — when the conditions were harder, when the tools were fewer, and when the personal cost was real.

INA Technologies Private Limited and its predecessor entity, INA Technology Solutions LLP, represent a sustained, structured commitment to the public WiFi access model. That commitment was made against significant headwinds: Jio's entry into the market compressed mobile data pricing to levels no one had anticipated, effectively rewriting the unit economics of subscription-based WiFi overnight. It was sustained through personal circumstances — including family health challenges — that would have given most people valid reason to pause. And it was made by choice: the founder brings 18 years of experience across enterprise organisations — TCS, Oracle, and TechMahindra — as well as independent consulting with MSMEs and startups, and the direct experience of building and running his own company. That path has always been available and has always been the easier option. The decision to build, and the decision to rebuild, has been deliberate at every stage. It is not driven by financial return alone. It is driven by conviction in what this model can do for the people it serves.

What we built:

The predecessor network OurFi (2016–2018) was a live, commercially operational public WiFi platform. 177 users confirmed in the independently generated Hotspot Express RADIUS report at the October 2017 snapshot, growing to approximately 190 confirmed in the platform's own application log across the full operational year, and approximately 250 over the full platform life. Real PayU-processed payments at Rs.15/GB — a price point that represented approximately one-tenth of prevailing broadband access rates at the time of launch. MikroTik routers, Hotspot Express RADIUS backend, a captive portal with an offers and marketplace layer. Users across locations. A two-sided platform that venue owners used to promote their businesses and that users relied on for affordable access.

The predecessor entity entered into a mutual non-disclosure agreement with a Fortune 500 semiconductor company in 2017 to explore a joint public WiFi

deployment model in India — demonstrating early enterprise validation of the concept at the ideation stage.

This was built bootstrapped, with no institutional funding, during the period when Jio's entry was compressing mobile data prices to a fraction of what they had been. That we launched, onboarded users, ran live payments, and secured a Fortune 500 partner in that environment is not a footnote. It is evidence of the kind of awareness, conviction, and execution that a transformative idea in a difficult market requires. The platform's own published statement at wind-down, still accessible at www.ourfi.in, notes close to 1 TB of cumulative data usage and participation from over a dozen venue operators — the founders' own published account of what the network achieved.

What we learned:

The platform ran for approximately 10–11 months of active operation. We documented what works: NPS of over 50 for seven consecutive weeks post-launch, a CAC of Rs.15, a 20% repeat rate, and the venue owner economic model — one operator reported a net monthly benefit of approximately Rs.2,200 once broadband cost savings and platform revenue were combined. We also documented what breaks: OTP failures in high-density environments, HTTPS captive portal limitations, session management gaps, and the absence of a regulatory framework that made data monetisation commercially viable at scale. These are not hypotheses. They are operational records from a live deployment.

> *Data note: The NPS figure, the repeat rate, and the "close to 1 TB" cumulative usage figure cited in this filing are based on information, operational records, and founder interviews conducted during version 1's operational period (2017). No formal measurement tool output is separately available. These figures are cited as directional indicators, consistent with independently verifiable operational data: 177 registered users confirmed in the Hotspot Express RADIUS report (October 2017), 152 GB total data confirmed in the same report, and Rs.344.69 in WiFi-specific PayU-processed payments confirmed via Axis Bank statements.*

What we are building now:

INA Technologies Private Limited, incorporated 20 May 2026, is aiming to rebuild R-Fi from the ground up — DPDP Act 2023 compliant from day one, with a separate Terms of Use and Privacy Policy, a single consent flow at onboarding, and optional personalised targeting consent within that flow, anonymised data monetisation as the primary revenue model, and PM-WANI as the operating framework. The rebuild is informed by months of structured, AI-assisted analysis of real version 1 operational data — session logs, user behaviour records, payment data, vendor API logs — and the current regulatory and competitive landscape. We are building in Telangana, in the exact market TRAI identifies as highest-potential and most underserved. We are not theorising about what this model can do. We are in the process of demonstrating it.

Why this matters beyond R-Fi:

UPI demonstrated that well-designed, regulation-backed digital infrastructure can compress class and geography barriers at national scale — and that India can lead the world in doing it. Public WiFi monetisation, properly structured under PM-WANI and DPDP, has the same potential. The connection event — a user joining a neighbourhood hotspot — is the moment where digital access, local commerce, and data value creation converge. When that moment is designed well, it serves the user, the venue owner, the data buyer, and the national digital agenda simultaneously. R-Fi is building toward that moment. This consultation is the regulatory foundation it needs.

7. The Moment, the Mission, and an Open Invitation

India's current conditions represent a convergence that has not existed before. The DPDP Act 2023, the PM-WANI framework, UPI's proven digital trust infrastructure, and the Government's sustained focus on MSMEs, digital startups, and Viksit Bharat 2047 are simultaneously active for the first time. Each alone creates opportunity. Together, they create the conditions for durable, scalable, inclusive public WiFi infrastructure.

This is not an assessment made from the outside. It is the view of a practitioner who has been building at the intersection of connectivity and data since 2006 —

and who attempted exactly this model in 2016, before this convergence existed.

Approximately 90 per cent of Indian startups do not survive beyond their first five years (IBM Institute for Business Value and Oxford Economics, 2021). The ones that return — with harder-won understanding, the same mission, and a policy environment that has finally caught up — represent a rare proof of sustained commitment. This filing comes from that group.

On approach — phased, data-driven, market by market:

Proliferation across India's markets — urban, semi-urban, and Tier 2 and beyond — will require a phased, marketing-data-driven rollout. Each market has its own infrastructure reality, consumer trust baseline, and operator incentive structure. Beginning with markets where demand is confirmed, trust barriers are measurable, and broadband capacity exists is not a conservative choice. It is the only approach that sustains momentum beyond the pilot stage. Broad national rollouts without data backing have failed before. Phased, evidence-backed expansion has not.

On the ecosystem — win-win, not zero-sum:

The goal this consultation is advancing is not a zero-sum competition between operators, telcos, or distribution channels. It is the creation of genuine win-win synergies and arbitrage across the entire ecosystem. Venue owners earn from idle broadband capacity and from promoting their own products and services through a proximity marketing channel that costs them nothing extra. End users access connectivity at a fraction of mobile data cost while receiving relevant, consent-gated offers at the moment they are most receptive. Data buyers receive privacy-compliant cohort insights unavailable through any other channel. Government achieves its Digital India and PM-WANI targets. TRAI demonstrates that regulation can catalyse new markets, not merely govern existing ones. INA Technologies Private Limited participates in this as a contributor to that shared value chain — not as an extractor from it.

An invitation to participate:

This response is a submission. It is also a request for collaboration — an invitation to work together toward the shared objective this consultation represents. The design assets, technical architecture, business documentation, and practitioner experience behind it are available to contribute beyond a written filing — through a TRAI working group, a PM-WANI pilot programme, or any consultative forum on PDOA governance and data monetisation. The lessons from version 1 — both what worked and what the regulatory gaps prevented — are the kind of ground-level input that policy frameworks benefit from. INA Technologies Private Limited looks forward to being a working participant in shaping that framework alongside TRAI and other stakeholders, not just a commentator on it.

A closing word:

At a time when many of this generation looked outward, the choice made here was always inward — to build in India, for this population, within this context. Not a career calculation. A conviction. The country's policy architecture and leadership are now at a point where that conviction meets its moment. India has already shown the world what is possible with UPI. What is being built here is the next layer on that foundation — the infrastructure that connects people to their neighbourhoods, their commerce, and their data rights, all at once. The timing for that contribution could not be better.

The formal responses below are grounded in the experience and observations described above.

We respond selectively to the questions most relevant to our operating context.

Part 2 — Formal Response

Submitted by: R-Fi / INA Technologies Private Limited

Contact: Rakesh Korumilli, Founder | rakesh.korumilli@gmail.com

Date: 25-May-2026

To: advbbpa@trai.gov.in | **CC:** jtadvbbpa-1@trai.gov.in

Section A — Status Assessment and Strategies for Public Wi-Fi Proliferation

Q4. What changes are required in the existing PM-WANI framework to improve revenue certainty and long-term sustainability for PDOs/PDOAs?

The PM-WANI framework has successfully lowered the registration barrier for community WiFi deployment — a well-designed foundation for neighbourhood-scale connectivity at scale. The consultation paper (paras 2.141–2.142) identifies multiple revenue models for PDOAs — direct revenue through paid access and advertising-supported arrangements, and indirect revenue through anonymised data analytics and footfall monetisation. Our version 1 operational experience (2016–2018) confirms that the model works when the full revenue architecture is in place. What constrains the ecosystem today is not the absence of a viable model, but the absence of clarity on how PM-WANI and the DPDP Act 2023 interact for data monetisation purposes.

The following changes would standardise, simplify, and unlock what is already latent in the PM-WANI ecosystem:

1. Clarify the regulatory interface between PM-WANI and the DPDP Act 2023 for data monetisation.
TRAI's consultation paper (para 2.142) identifies anonymised footfall and usage data as a potential PDOA revenue stream. PM-WANI is currently a connectivity framework — it does not address data monetisation. The DPDP Act 2023 governs consent and data processing but currently

operates as a separate regulatory track with no published guidance on how it applies to PM-WANI PDOAs. A joint TRAI-MeitY clarification — explicitly connecting PM-WANI and DPDP, and confirming how consent obligations apply within a PM-WANI operating context — would allow PDOAs to design compliant systems with confidence, engage data buyers commercially, and attract investment. This is a chance and opportunity for clarity, standardisation, and communication.

2. Standardise minimum data retention and API interoperability for PDOAs.

Currently there is no standard for what session data a PDOA must collect, retain, or make available. This creates fragmentation that makes compliance harder and ecosystem development inconsistent. A baseline interoperability standard — session timestamps, data volume, device type, no PII — would reduce compliance friction, allow tools and integrations to be built once and used across the ecosystem, and ensure consistency without constraining PDOAs to a single architecture.

3. Introduce performance-linked revenue sharing from government-funded backhaul.

Where the government funds BharatNet or DBN backhaul used by PM-WANI hotspots, a small percentage of the cost saving should be rebated to the PDOA as a sustainability subsidy for the first 24 months. This removes the chicken-and-egg problem where PDOAs cannot survive long enough to build user density.

4. Streamline PDOA onboarding for Startups and MSMEs.

Current PDOA registration requires engagement with C-DoT's central registry, which is designed for large ISPs. A simplified, self-serve digital onboarding path for startups, MSME entities, and other small operators — including Startup India-registered entities — would meaningfully increase PDOA participation from this sector.

Q5. Are there any other challenges currently faced by PDOAs/PDOs? What changes can enhance participation of

entrepreneurs under PM-WANI?

Drawing on the direct operational experience of our predecessor network OurFi (2016–2018), which ran live hotspots before the PM-WANI framework was formalised, the challenges are:

1. Authentication friction destroys user retention.
India's DoT 2009 OTP mandate requires per-session mobile number verification. In dense areas — markets, train stations, events — cellular congestion delays or drops OTPs entirely, causing failed logins. In our predecessor network's version 1 deployment (OurFi, INA Technology Solutions LLP), some users logged about 19 sessions in a single day, most lasting under 60 seconds, because OTP failures prevented successful session establishment — users logging multiple short sessions in a single day being the clearest indicator of OTP friction in the data. Auto-relogin via MAC address cookie would have eliminated this. TRAI should clarify that auto-relogin — without requiring a fresh OTP for returning devices within a defined window — is permitted and does not violate the 2009 directions. A specific practitioner insight from version 1 operations illustrates the broader case for published operational standards: implementing a delayed OTP resend — where the resend option activates only after 30 seconds and sends a fresh OTP rather than the original — meaningfully reduced OTP failure rates in our deployment. Users who encountered a failed first delivery completed login on retry rather than abandoning. This improvement was discovered through deployment experience, not from any published reference document. Without such a document, every PDOA entering the ecosystem must rediscover it independently — with their early users absorbing the cost of the learning curve.

2. No standard commercial framework between PDOAs and hardware/RADIUS vendors.
PDOAs depend on vendor agreements that have no standardised terms. Our version 1 contract with Hotspot Express was bespoke, undocumented in key areas, and tied to the specific LLP entity — not transferable to a

successor company. DoT or TRAI should publish model contract templates for PDOA-vendor agreements, covering API access rights, data portability, and entity transfer provisions.

3. Data ownership and continuity gaps when PDOA entities restructure.

A structural vulnerability exists in bootstrapped PDOA startups that has no current regulatory answer: when co-founders separate — as frequently happens in early-stage ventures, driven by cost pressures, time constraints, diverging priorities, and general life circumstances — there is no established framework for what happens to network infrastructure, customer data, vendor contracts, and operational continuity. Data collected under a PDOA registration has no clear ownership or continuity framework when the operating entity restructures. INA Technologies' predecessor entity experienced this structural gap directly.

Government should be a stakeholder in this data, not merely an overseer. Public data collected over public-access networks has a public accountability dimension that goes beyond private partnership disputes. We recommend TRAI consider the following options — not mutually exclusive:

- **(a) Data Controller Designation:** PDOA registrations include a named Data Controller whose designation survives entity changes. The Data Controller retains access rights and responsibility even if the underlying entity restructures or partners separate. This is the cleanest solution but may require ongoing government resources to administer at scale.
- **(b) Data ownership tied to shareholding and Companies Act:** User data is treated as a proportional asset of the registered entity under company law, with the government holding a defined co-custodian interest and a revenue participation right in commercial data monetisation. This ties data governance to existing corporate law without requiring new infrastructure.

- **(c) Mandatory data escrow above a user threshold:** PDOAs with more than a defined number of registered users must place operational data with an encrypted, third-party custodian — accessible only under defined conditions such as partner dispute, entity dissolution, or regulatory requirement.

INA Technologies Private Limited, as a PDOA operator with direct experience of this structural gap, would welcome the opportunity to contribute to any TRAI consultation specifically on PDOA data governance and continuity frameworks.

4. The "free Wi-Fi expectation" is a legitimate market distortion that needs a policy response.
Government-funded free Wi-Fi deployments (Hy-Fi in Hyderabad, RailTel at stations) have trained urban consumers to expect zero-cost access. Private PDOAs cannot compete with this. TRAI should publish guidelines distinguishing "public access" deployments (government-funded, free, universal) from "commercial hotspot" deployments (private, subscription or ad-funded) to allow both to coexist without the former destroying the economics of the latter.

Section G — Technical Architecture, Authentication, and Interoperability

Q22. Are users facing challenges with authentication and authorisation procedures? How can processes be simplified while ensuring security and compliance?

Yes. The challenge is structural, not incidental.

India's current Public Wi-Fi authentication is governed by DoT directions from 2009 — before smartphones were mainstream, before UPI existed, and before PM-WANI was conceived. Applied to mobile, high-footfall,

multi-session Wi-Fi environments in 2026, it creates three specific failure modes:

Failure mode 1: OTP delivery failure in high-density environments.
At markets, malls, and transport hubs — precisely where public Wi-Fi has the most value — cellular networks are most congested. OTP delivery fails or delays by 30–120 seconds. Users abandon the connection attempt. This is the primary cause of sub-1-minute sessions in our version 1 data.

Failure mode 2: Per-session re-authentication for returning users.
A user who authenticated last Tuesday is forced to re-authenticate today. There is no persistent device trust. This eliminates the "habitual reliance" that the Consultation Paper (para 2.140) identifies as critical to shifting mobile data consumption to Wi-Fi.

Failure mode 3: HTTPS interception failure.
The current captive portal architecture requires intercepting an HTTP request. Modern devices default to HTTPS. HTTPS cannot be intercepted without generating a certificate error. Mobile browsers treat certificate errors as security threats and block the connection. This means users on iPhones and Android 9+ cannot even reach the captive portal — a known limitation documented in our predecessor network's version 1 deployment.

Recommended approach:

a) **Permit MAC-cookie based auto-relogin for registered returning devices.** A device that has successfully authenticated via OTP within the past 30 days should be granted automatic session resumption via secure MAC cookie. This is already technically implemented in most hotspot platforms (including MikroTik) but the 2009 DoT directions require per-session authentication and provide no exception for verified returning devices. An explicit TRAI recommendation to DoT permitting auto-relogin within a defined window would unlock this without requiring new legislation. MikroTik's hotspot platform includes cookie-based session

handling as a configurable feature. During version 1 operations under the predecessor entity (OurFi, INA Technology Solutions LLP), we tried and experimented with different return authentication approaches — varying session timeout settings, OTP resend flows, and connection resumption methods. Based on this experimentation, our assessment is that MAC cookie combined with auto-relogin — where a returning verified device rejoins without a fresh OTP — offers the most reliable and friction-free return experience for users at the same hotspot. Cross-hotspot sessions — moving from one PDO location to another — still required full re-login each time. This is precisely the friction gap Passpoint/Hotspot 2.0 closes at the network protocol level. The practical sequencing: resolve the single-hotspot return experience first (MAC cookie, regulatory clarity), then build the infrastructure for seamless cross-hotspot roaming (Passpoint glide path).

b) **Permit UPI ID as an authentication credential.** A UPI VPA is tied to a KYC-verified mobile number. Authenticating via UPI collect flow provides identity verification equivalent to OTP without cellular congestion dependency. NPCI and DoT should jointly define a standard for this.

c) **Adopt Passpoint/Hotspot 2.0 as the long-term standard — but with a 24-month glide path, not an immediate mandate.** Passpoint/Hotspot 2.0 eliminates captive portals entirely. Authentication happens at the 802.1X layer — no browser redirect, no HTTP interception, no HTTPS problem, no per-session re-auth. MikroTik hardware already supports this via firmware upgrade. However, Passpoint requires enterprise-grade RADIUS (FreeRADIUS or equivalent), 802.1X certificate infrastructure, and device-side credential provisioning — none of which a small PDO can deploy at launch. Mandating Passpoint as a registration requirement today would create a technical and financial barrier that eliminates small PDOAs before they start, concentrating the market in large players who can afford the infrastructure. The right policy is a glide path: launch on captive portal (Track 1), graduate to Passpoint (Track 2) as

the platform scales. R-Fi's own architecture is built on exactly this two-track sequence. TRAI should set a 24-month compliance window for new registrations, not an immediate mandate — this is detailed further under Q26.

Q23. Is there a need for a centralised platform for authentication and payment systems? Which entity is best suited?

Yes, with caveats.

- **Authentication:** C-DoT is the appropriate technical custodian. The platform should be an API, not a portal — so PDOA captive portals can call it natively without redirecting users to a government website.
- **Payment:** NPCI via UPI. The payment and identity functions should be unified — a single UPI-based flow that simultaneously verifies identity and optionally processes payment.
- **Data:** No centralised data collection. Session metadata should remain at the PDOA level, collected under DPDP-compliant consent frameworks. Centralising data creates a single point of breach risk and concentrates market power in ways that disadvantage small PDOAs.

Section H — Monetisation and Sustainability

Q25. What monetisation models are most appropriate for rural, urban, and high-footfall locations?

Rural:
The free-access-with-government-subsidy model is appropriate where income levels and digital literacy make subscription models unviable. The sustainable path: government funds backhaul (BharatNet/DBN), PDOA provides last-mile access at zero cost to users, and PDOA is compensated via viability gap funding tied to uptime SLAs. Secondary revenue should

come from government digital service delivery (e-governance, DBT verification) rather than commercial data sales.

Urban (semi-urban / Tier 2):
The PM-WANI model is well suited to a freemium approach in semi-urban and Tier 2 markets — limited free access as a customer acquisition mechanism, with paid upgrades for extended access. Our predecessor network's version 1 operational experience in Hyderabad confirmed that the prepaid, per-use data access model works at this tier — real payments at Rs.15/GB, real users, real session data. The conceptual foundation for data monetisation was also built and tested: per-venue analytics were operational, giving a venue-centric view of footfall and session behaviour, and the offers layer was live with over a dozen venue operators running branded content to every connecting user (per the platform's own published statement at wind-down; figures are directional). The data buyer revenue stream was not commercially live in version 1 — the regulatory framework and commercial infrastructure for that did not exist pre-PM-WANI. That is precisely what clarity on PM-WANI and DPDP unlocks. The revenue architecture that works in practice:

- A single DPDP-compliant consent flow at onboarding — supported by a separate Terms of Use and a separate Privacy Policy — covers all data uses: anonymised session analytics (active by default, required for the service) and personalised commercial targeting (clearly optional; WiFi access is never conditioned on this consent). This structured approach works under DPDP when designed thoughtfully into the user journey.
- Anonymised cohort data buyers: fintechs (credit scoring), FMCG brands (cohort targeting), quick commerce (footfall heatmaps), offline retail (dwell time analytics), real estate developers (catchment analysis).
- Practitioner evidence: the arbitrage between the marginal cost of serving a connected user and the value of consented, location-anchored behavioural data is the sustainable engine for PDOA economics at this tier. Version 1 confirmed the unit economics of per-use data access and

the conceptual architecture of the data layer; comparable global markets confirm the data buyer revenue model at scale.

High-footfall (urban, captive):
Advertising-supported free access is the dominant global model and well suited to India's high-footfall locations. The captive portal login screen is a natural ad placement surface — value that already exists in every deployed hotspot. A standardised revenue-sharing framework between venue PDOs, PDOAs, and ISP backhaul providers would remove negotiation friction, make the economics predictable, and give venue owners a clear reason to participate. TRAI publishing an indicative template — even as a starting point for industry-led refinement rather than a mandated split — would accelerate ecosystem self-organisation significantly.

Additional model — Hyperlocal venue marketing:
In semi-urban and neighbourhood settings, the captive portal is a local commerce channel. The mechanism is straightforward: each deployed router is registered to a venue owner with a unique location identifier. When any user connects at that location, the R-Fi server uses that identifier to look up the venue's chosen template (gym, café, bakery, etc.) and the offers the owner has configured in the back-office management panel. The post-authentication screen serves that venue's branded content to every connecting user before they reach the open internet — zero additional cost to the venue owner, zero friction for the user, and a direct marketing channel tied to physical footfall. version 1 OurFi operated this system with over a dozen venue operators across multiple business categories in 2017. A gym owner, a café, a bakery, a training centre — each had their own branded screen and their own offers. It drove location owner participation directly: venue owners had a tangible reason to host a router beyond the broadband cost offset. TRAI should explicitly recognise hyperlocal venue marketing as a permitted PDOA revenue-sharing activity, with DPDP-compliant disclosure requirements built into the platform consent flow.

version 1 practitioner evidence — per-venue analytics were live, not theoretical:

OurFi — our predecessor network, operated under INA Technology Solutions LLP — version 1 (2017) operated two parallel analytics views at the platform level: a user-centric view (all sessions by a phone number across any location) and a venue-centric view (all sessions through a specific device/router by any user). The venue-centric view is the foundation of what data buyers will pay for — footfall counts, dwell time, and user cohort behaviour at a named location. This dual-view architecture was confirmed operational in production during version 1 testing, sourced from developer QA records. The data monetisation model this consultation is examining is therefore not speculative — it was built, tested, and in use in Hyderabad in 2017, before PM-WANI was formalised. Regulatory clarity is the missing piece, not technical readiness or commercial viability.

Q26. Additional comments and observations

1. The DPDP Act 2023 is conspicuously absent from this consultation.

The Consultation Paper's Section D.5 discusses anonymised data monetisation without once mentioning India's own data protection legislation. Any PDOA considering data monetisation in 2026 must design for DPDP compliance from day one. TRAI should issue supplementary guidance clarifying how DPDP obligations apply to PDOs and PDOAs, and what the interaction is between the PM-WANI framework (DoT) and the DPDP Act (MeitY).

2. OpenRoaming should be planned for, not mandated immediately.

TRAI should set a 24-month glide path: new PDOA registrations from 2027 onwards must be Passpoint-capable; existing PDOs have until 2028 to upgrade via firmware or replacement (with viability gap funding support).

3. Telangana's semi-urban Tier 2 gap is not addressed.
The Hy-Fi deployment demonstrates what state government-led urban Wi-Fi can achieve (3,000+ hotspots). But Telangana has 31 districts with over 100 towns of 50,000–5,00,000 population that have no comparable coverage. TRAI should recommend that state governments create Tier 2 Wi-Fi zones with simplified RoW clearances, reduced spectrum fees, and fast-track PDOA registration.

4. The "super-aggregator" model for roaming (Q24) risks market consolidation.
A mandatory super-aggregator would concentrate gateway power in one entity and create a toll-booth for all PDOA revenue flows. We recommend a federated model — PDOAs opt into roaming agreements bilaterally or via voluntary consortia — modelled on the OpenRoaming WBA framework.

5. Publish a PDOA operational best practices reference guide — for all ecosystem participants.
A significant and largely invisible barrier to ecosystem penetration is the absence of published operational guidance for PDOAs and their stakeholders. OTP handling, session management, captive portal compatibility, consent flow design, data retention practices — each involves configuration choices that directly affect user experience and compliance, but none are documented in any reference a new PDOA can easily access. Operators currently learn through deployment experience, meaning their early users absorb the cost of every learning curve. TRAI or DoT publishing a plain-language operational reference guide — covering technical standards, user-facing dos and don'ts for each stakeholder group (users, hotspot owners, data buyers), and compliance checklists — would compress that learning curve for every new entrant and meaningfully improve early user experience across the ecosystem. This does not require new regulation. It requires documentation of what already works, made accessible to everyone who needs it before they start.

Closing Note

The consultation paper asks the right technical and regulatory questions. But the practitioner evidence points to a more fundamental barrier: **awareness**. Infrastructure exists. Regulation is evolving. The model works. What is missing is a shared understanding — among users, device owners, local businesses, and policymakers — of what a well-designed public Wi-Fi platform actually does and for whom.

The core need is straightforward: fast, affordable, good quality internet access. This is what users want, and what they will pay for when it is available and trustworthy. Public WiFi — and PM-WANI specifically — is structurally well-suited to deliver exactly this, at a fraction of mobile data cost, using infrastructure that already exists in millions of Indian homes and businesses. R-Fi is built to deliver on this need.

Our own primary survey (63 respondents, Hyderabad, Dec 2025) confirms the demand signal:

- Speed is the single most important factor in a secure WiFi connection — 68% rated it Most Important or Very Important
- Cost savings is the #1 reason users would choose OurFi — 60% named it as their top reason
- Plan validity ranks third — users want access that lasts, not connections that expire mid-use
- R-Fi's model directly addresses all three

Three awareness gaps operate simultaneously: users do not know what they are entitled to; device owners do not know what they are sitting on; and policy has not yet named the integrated model. R-Fi has built and operated this model. We are submitting this response to name it clearly.

What government can do:

- Publish a plain-language user-facing standard: what a PM-WANI PDOA can and cannot do with your data
- Introduce a visible "DPDP Compliant" certification marker for hotspots — analogous to BIS marking on electronics
- Name data monetisation and hyperlocal commerce explicitly as intended, desirable ecosystem outcomes of PM-WANI — and connect PM-WANI with the DPDP Act 2023. TRAI's consultation paper identifies these as potential revenue streams; a joint TRAI-MeitY communication that connects the two frameworks and tells every ecosystem participant what they can build with confidence is what accelerates adoption
- Enable standardised revenue sharing between PDOAs and device owners — removing negotiation friction is what makes the model self-propagating, not dependent on subsidy

Why R-Fi is the right voice: We ran a live network in Hyderabad from 2016–2018 — 177 users confirmed via independently generated RADIUS records (October 2017 snapshot), 190 users confirmed via our own application log (Jan–Dec 2017), growing to approximately 250 users over the full operational period. Real PayU-processed payments, users across locations. Critically, we did not just count users — we built and operated per-venue analytics: a live system that tracked all users at each hotspot location separately from user-level activity. The venue-centric data layer, which is the foundation of the data monetisation model TRAI is now consulting on, was functional in our 2017 system. We encountered and solved the real operational challenges: ISP cascading portals, HTTPS captive portal failures, session timeout behaviour, payment reconciliation, consent design. R-Fi is being rebuilt DPDP-compliant from day one, incorporating all of these lessons. We are building in the exact market this consultation identifies as highest-potential and most underserved. The awareness argument is not abstract for us. It is the lesson we learned the hard way and are now positioned to act on.

Summary of Key Recommendations

Recommendation	Question	Priority
Clarify PM-WANI / DPDP regulatory interface for data monetisation (para 2.142 identifies it as a potential revenue stream — PM-WANI and DPDP must be explicitly connected through joint TRAI-MeitY standards and communication)	Q4, Q25	**Critical**
Issue joint TRAI-MeitY guidance on DPDP Act interaction with PM-WANI	Q26	**Critical**
Address the awareness gap — government naming and promoting the integrated model	Section I	**Critical**
Permit MAC-cookie auto-relogin for returning authenticated devices	Q22	**High**
Define UPI VPA as a valid authentication credential	Q22	**High**
Publish model PDOA-vendor contract templates	Q5	**High**
Set 24-month Passpoint/Hotspot 2.0 glide path for new registrations	Q26	**Medium**
Create Tier 2 Wi-Fi zones with simplified RoW for private PDOAs	Q26	**Medium**
Publish standard revenue-sharing template for high-footfall locations	Q25	**Medium**
Avoid mandatory super-aggregator; use federated roaming model	Q24	**Medium**

Publish PDOA operational best practices reference guide for all ecosystem participants	Q26, Q5	**Medium**