Comments in response to the TRAI's Consultation Paper on the "Proliferation of Public Wi-Fi Networks in India" dated 27.04.2026

1. The following comments are based on the perspective that the right to access the internet ought to be a fundamental right. The Hon'ble High Court of Kerala in *Faheema Shirin R.K. v. State of Kerala, WP(C).No.19716 of 2019(L)*, judgment dated 19.09.2019 has noted that "the right to have access to Internet becomes the part of right to education as well as right to privacy under Article 21 of the Constitution of India". The Hon'ble Supreme Court of India in *Anuradha Bhasin v. Union of India, AIR 2020 SC 1308*, noted that access to the internet is necessary for the exercise of fundamental rights under Article 19(1)(a) and Article 19(1)(g) of the Constitution of India. Recently, the Hon'ble Supreme Court of India in A*mar Jain v. Union of India W.P.(C) No. 49/2025 and Pragya Prasun v. Union of India, W.P.(C) No. 289/ 2024*, also noted that right to digital access is an instinctive component of the right to life and liberty, necessitating that the state proactively designs and implements an inclusive digital ecosystem that serves not only the privileged but also the marginalized and those historically excluded.

2. Public Wi-Fi could be one of the requisite technological changes that can help us further universal access to the internet as a fundamental right.

A. Issues in the proliferation of Public Wi-Fis

3. There are several structural constraints that impede the wide-spread adoption of Public Wi-Fi networks in India.

4. From the user's side, the cheap costs of mobile data has meant that the experience of using the internet throughout the day is seamless and always available. In contrast, Public Wi-Fi networks often require manual authentication, log in, and/or purchase of vouchers. These are both operational and financial impediments to the adoption of Public Wi-Fi networks. Thus, actual usage of Public Wi-Fi remains quite low because of the need to "switch" from mobile data to Public Wi-Fi. An average user getting a mobile data package for 2 GB/day is already paying 490 per month just for mobile data (See Annexure - 1 of Consultation Paper). This may be in addition to broadband connection at home. When existing mobile data packs available for the day have not been exhausted by users, Public Wi-Fi that is available even for a small cost seems wasteful.

5. For Public Data Offices if only a handful of customers everyday pay the voucher cost for hotspots, it is insufficient to cover recurring expenses of PDOs, such as backhaul bandwidth charges.

6. For Internet Service Providers, data offloading from licensed spectrum services to Wi-Fi operating on unlicensed spectrum may be of benefit to ease network congestion. However,

they prioritise delivering quality broadband services to their own customers at affordable rates before considering any price cuts for outsiders such as PDOs who are involved in provision of Public Wi-Fi. However, PDOs / hotspot providers which are typically shop owners and commercial establishments would want to purchase broadband connection for Public Wi-Fi at costs that they can recoup at. Moreover, as indicated above, most users would want Public Wi-Fi to be free and thus, PDOs may not be able to recoup their expenses paid towards TSPs in accessing backhaul infrastructure and services from TSPs for Public Wi-Fi. As indicated by Reliance in its comments to TRAI's Telecommunication Tariff (Seventy First Amendment) Order, 2025,[1] TSPs are vehemently opposed to providing backhaul services to PDOs because they believe it forces TSPs to sell their network services to a competitor service (PDOs offering public Wi-Fi) at cheaper prices. They also insist that any commercial arrangements including tariffs between the PDOs/PDOAs and TSPs should be left to the "market forces". However, these proposals leave much open to the whims of market forces.

7. We note that in respect of the PM-WANI scheme, deployment friction has been sought to be reduced by two measures. First, on 16 September 2024, DoT issued amendments to the PM-WANI framework by removing the requirement for PDOs to enter commercial agreements with TSPs for internet connectivity and permitting PDOs to network up to 100 access points to establish a single Wi-Fi hotspot.[2] Second, the Telecommunication Tariff (Seventy First Amendment) Order, 2025 has already stated that "*every service provider providing retail Fiber to the Home (FTTH) broadband services shall offer all of its retail FTTH broadband plans upto 200 Mbps to the PDOs under the PM-WANI scheme, at tariff not exceeding twice the tariff applicable to the retail subscribers for the corresponding FTTH broadband plan of the bandwidth (capacity) offered*".[3] These changes should be extended to Public Wi-Fi schemes and frameworks outside the PM-WANI scheme as well.

8. Based on a survey of the issues that impede broad adoption and proliferation of Public Wi-Fi network services, we recommend the following:

    a. TRAI must recommend that PDOs should be able to use broadband on fixed line connections at a cheaper tariff rate rather than leased-line tariff rates. TRAI must also indicate the tariff rate at which TSPs/ISPs can offer backhaul to PDOs. Unlike what the TSPs/ISPs may recommend, it is important that the introduction and uptake for Public Wi-Fis is carefully administered with governmental oversight over ease of access and costs.

[1] Reliance Jio Infocomm Limited, RJIL's comments on TRAI's Draft "The Telecommunication Tariff (71st Amendment) order, 2025", RJIL/TRAI/2024-25/329, 31 January 2025, available at: https://www.trai.gov.in/sites/default/files/2025-01/RJIL_31012025.pdf.
[2] DoT, Data Services Cell, Amendments/Additions in Wi-Fi Access Network Interface (WANI) Framework and Guidelines for Registration, File No. DS-16/13/2017-DS-III(Vol-II), dated 16.09.2024.
[3] Telecommunication Tariff (Seventy First Amendment) Order, 2025, dated 16 June 2025.

b. To convince shop owners and commercial establishments to have public Wi-Fi, not only must the tariff be cheaper, but public messaging on the fact that this may enhance their business would be necessary. Internet access in shops and cafes have become a necessity and businesses that have public Wi-Fi may attract more consistent customers than otherwise.
c. Governments at the state-level and local level ought to help PDOs obtain right of way permissions swiftly. They can also introduce short-term projects that integrate street furniture (such as lamps, bus stops) for enhancing Wi-Fi availability.
d. In rural areas, certain public offices and public infrastructure such as bus stops, schools, police stations, Anganwadis, administrative offices of the village, libraries ought to have Public Wi-Fi access points. This can then be expanded to other areas including shops and commercial establishments in and around the village. In remote areas, where cables are difficult to install, the government should consider supporting satellite internet access for these public access points for Wi-Fi.
e. For enhancing both outdoor and indoor access of Public Wi-Fi, signalling that unlimited or limited free Wi-Fi as the case may be available would be necessary. Public and commercial establishments often do not provide an indication that Wi-Fi is available, and so a board that says how to access it would be helpful.

B. Existing PM-WANI Framework

9. The PM-WANI framework was introduced with the objective of creating a decentralised and low in cost public Wi-Fi ecosystem. The framework represents the Government's flagship initiative for Wi-Fi proliferation which adopts an app-based hub in order to reduce entry barriers, encourage participation by small entrepreneurs, and promote competition. Further, by permitting PDOs to provide public Wi-Fi access without obtaining a separate licence, registration, or payment of fees to the DoT, the framework sought to enable small shops, local businesses, and community-level institutions to participate in expanding internet access. In theory, this model could help create a distributed layer of last-mile connectivity, particularly in areas where fixed broadband access is limited or where mobile data remains either unreliable or insufficient.

10. However, it is noted that scaling the number of public hotspots across diverse geographies, especially in remote and underserved regions remains uneven. This could be telling of the fact that in practice, a PDO must still incur costs for broadband connectivity, routers, maintenance, customer support, and compliance-related requirements, while knowing that user willingness to pay for public Wi-Fi is uncertain. Therefore, the central issue here could be the fact that the PM-WANI framework assumes that public Wi-Fi can be sustained primarily through market-led participation. This assumption may not hold in many contexts. For example, in urban areas, users may already have access to inexpensive mobile data and may not shift to public Wi-Fi unless it is free, faster, more reliable, or easier to access. And as mentioned above, in rural, semi-urban or remote and underserved regions, where

public Wi-Fi may serve a stronger inclusion function, the ability of PDOs to recover costs from users may be even more limited. Therefore, the framework requires a more active facilitative role from the government, rather than fully relying only on PDO-level entrepreneurship.

11. The DoT's amendment to the Telecommunication Tariff (Seventieth Amendment) Order, 2024 dated 16 September 2024 appeared to recognise some of these difficulties. By removing the requirement for PDOs to enter into commercial agreements with TSPs for internet connectivity, the amendment reduces friction under the PM-WANI framework. This means that, under the scheme, PDOs (anything from a kirana store to a tea shop) can operate Wi-Fi hotspots without paying a license fee or undergoing a registration process. Further, the seventieth amendment also allowed PDOs to take internet connectivity at a single point (like a mall, bus station, etc) and can network up to 100 access points to create a single Wi-Fi hotspot. This means that they can cover large areas, such as different floors of a mall, a large market, or a big complex, eliminating dead zones. This allowed better connectivity in widespread areas.[4]

12. Similarly, the Telecommunication Tariff (Seventy First Amendment) Order, 2025, requires service providers offering retail FTTH broadband plans up to 200 Mbps to offer such plans to PDOs at tariffs not exceeding twice the tariff applicable to retail subscribers, is a useful intervention.[5] These measures recognise that backhaul access and tariff certainty are central to the viability of public Wi-Fi networks. However, these measures should be treated as a starting point rather than a complete solution. If PDOs continue to face high recurring costs, uncertainty in commercial arrangements, lack of technical support, and low user willingness to pay, the PM-WANI framework will remain underutilised. TRAI should therefore recommend that the framework be strengthened through local government support.

13. We recommend the following:
    a. TRAI should examine whether the "twice the retail tariff" ceiling is sufficiently affordable for small PDOs, especially in low-income and rural areas where user revenue may be limited.
    b. PM-WANI should be made more user-facing and discoverable. A major barrier to adoption is that users often do not know whether public Wi-Fi is available, how to access it, what it costs, or whether it is reliable. Public and commercial establishments offering PM-WANI access should be encouraged to display clear signage indicating the availability of Wi-Fi, applicable charges, free access limits, and

[4] Kamya Pandey, "India Relaxes Public Wi-Fi Rules: Small businesses Can Now Operate Wi-Fi hotspots Without Commercial Agreement", MediaNama, 18 September 2023, available at: https://www.medianama.com/2024/09/223-dot-amends-pm-wani-guidelines-pdos-wifi-hotspots-without-commercial-license/

[5] Telecom Regulatory Authority of India, "Information Note to the Press (Press Release No. 46/2025)", 16 June 2025, available at: https://www.trai.gov.in/sites/default/files/2025-06/PR_No.46of2025.pdf

the mode of authentication. This is necessary to convert hotspot availability into actual usage.

c. Further, as also highlighted below, public Wi-Fi systems and networks across the world are construed as less secure than mobile data or private broadband connections. A baseline set of technical and security standards should be set, insofar as they are technically feasible with Public Wi-Fi provisioning. Websites that concern financial, medical, or other sensitive personal data should be expected to alert its users that they are on a public network that is less secure than mobile data.
d. A purely paid model may fail to attract users who already have mobile data or exclude those who need public Wi-Fi the most. Therefore, we recommend that PM-WANI not be designed only around paid access models.
e. Further, we recommend that the PM-WANI framework be strengthened through clearer data protection and security safeguards. The present framework contains only a broad obligation on App providers, Central Registry Providers and PDOAs to safeguard privacy. This is insufficient for a framework that may involve authentication details, device identifiers, session information, payment records, and location-based access. TRAI should recommend detailed safeguards on data collection, retention, sharing, deletion, security, and grievance redressal across the PM-WANI ecosystem.
f. TRAI must ensure that PM-WANI serves the broader objective of meaningful and inclusive internet access

C. Authentication to access Public Wi-Fi

14. The Department of Telecommunications, through its order dated 23.02.2009, had noted that unsecured Wi-Fi networks could be misused without leaving a traceable trail of users. On this basis, DoT directed public Wi-Fi providers to follow an authentication procedure before allowing access to users.[6]

15. However, as pointed out in our earlier submission,[7] TRAI must first examine whether the present authentication framework remains necessary, proportionate, and effective. The 2009 directions appear to have proceeded from a generalised concern that Wi-Fi networks may be misused by anti-social elements. They were not preceded by a public consultation, background paper, technical study, or risk assessment that demonstrated why user authentication was the appropriate regulatory response. Subsequent developments in this area have also largely proceeded without meaningful consultation with experts, civil society, or the general public. Given that authentication requirements directly affect access, privacy,

[6] Government of India, Ministry of Communications & IT, Department of Telecommunications, Letter with Subject Line "Instructions under the UASL/CMTS/BASIC Service Licence regarding provision of Wi-Fi Internet service under delicensed frequency band", 23 February, 2009, available at: <https://www.airwaybroadband.com/pdf/Wi-%20fi%20Direction%20to%20UASL-CMTS-BASIC%2023%20Feb%2009.pdf>

[7] Internet Freedom Foundation, Comments on TRAI's Draft "Consultation Note on Model for Nationwide Interoperable and Scalable Public Wi-Fi Networks", 09 December, 2016, available at: <https://www.trai.gov.in/sites/default/files/2024-11/Internet_Freedom_Foundation.pdf>

and exclusion, this issue requires closer study by TRAI before any further regulatory framework is recommended.

16. Further, the Consultation Paper itself recognises that public Wi-Fi authentication in India presently relies on an SMS-based OTP verification or physical/photo identity documents that may be retained for audit purposes. While this model may have been introduced to ensure traceability, it creates significant operational friction. Users are required to manually authenticate themselves for each session, simultaneous logins through the same credentials are restricted, and access often depends on the availability of a working mobile connection.

17. Moreover, TRAI also noted that while the introduction of the PM-WANI framework in December 2020 marked a methodological shift by enabling registration-based deployment of Public Wi-Fi access points, PM-WANI did not fundamentally change the authentication mechanism. The dependence on SMS-based OTP for first-time authentication introduces operational friction, TRAI noted that OTP delivery may be delayed in high-density environments because of cellular network congestion. This creates a contradictory situation where users may require mobile connectivity in order to access Wi-Fi, even though public Wi-Fi is meant to serve as an alternative and additional layer of internet access.

18. If public Wi-Fi introduces such SMS-based OTP or registration frameworks, it would not merely become a matter of inconvenience but also affect public Wi-Fi adoption. Therefore, TRAI should recommend moving away from OTP-based authentication as a default model for access to Public Wi-Fi.

19. TRAI's Consultation Paper discusses contemporary authentication methodologies such as Passpoint/Hotspot 2.0, which use 802.1X/EAP-based provisioning to enable automatic and secure connectivity without repeated user intervention. It also notes that public Wi-Fi roaming in India remains largely ISP-specific and fragmented, while global standards such as OpenRoaming are increasingly being adopted for interoperable roaming. Such models can improve user experience and reduce repeated login friction, especially in high-footfall public spaces. This could also reduce the need for repeated data sharing with various public Wi-Fi providers.

20. The shift to seamless authentication should not be used to normalise intrusive identity verification. Any recommended authentication model must be designed to minimise repeated data sharing and prevent centralised profiling. TRAI should therefore ensure that seamless access is accompanied by clear privacy safeguards, including data minimisation, purpose limitation, storage limitation, transparency, security safeguards, and meaningful user choice. Importantly, it must be noted that public Wi-Fi is an access-enabling infrastructure.

21. Further, TRAI's discussion on integrating UPI for authentication and payments also requires caution. While UPI may reduce payment friction and improve the commercial viability of

public Wi-Fi networks, payment integration should not become a substitute for identity verification or a means of profiling users. Any UPI-linked model must preserve user choice, allow non-UPI alternatives such as vouchers or free access models, and avoid creating centralized records that combine identity, payment, location, and browsing-session metadata.

22. Proliferation of broadband through Wi-Fi hotspots is impossible if TRAI insists on a mechanism that places undue emphasis on authentication and KYC norms. Further, the guidelines for the PM-WANI scheme only discuss data protection in a cursory manner, stating that PDOAs shall "take all necessary steps to safeguard the privacy and confidentiality of any information about a third party to whom it provides the service" (Para 4(c)). TTRAI should therefore recommend detailed obligations on data collection, retention, deletion, cybersecurity, and grievance redressal for all entities involved in the public Wi-Fi ecosystem.

23. We recommend the following:
    a. TRAI should recommend a shift away from SMS- based OTP authentication for public Wi-Fi.
    b. Authentication should not become mandatory KYC for internet access.
    c. If authentication is necessary, it should comply with the existing data protection framework. Further, TRAI can recommend a separate security framework for public Wi-Fi.

D. Governance models that would be best suited for proliferation Wi-Fi

24. Given that ISPs prioritize their commercial viability over widespread installation and adoption of Public Wi-Fi systems, it is critical that the governance model adopted involves more active Government oversight over commercial entities like ISPs. The Central Government and state governments must also assist in hotspot deployment through direct funding and implementation support through DPOs, including providing assistance in backhaul provision.

25. We recommend that the government assumes different funding and facilitative roles based on where the Public Wi-Fi is installed:
    a. Self-deployment is recommended for public institutions like schools, libraries, parks, offices that are administered by the government.
    b. Targeted interventions in private institutions where installing Public Wi-Fi can enhance coverage. This could be by direct funding of the installation of backhaul infrastructure while the operational costs are covered by the commercial establishments / DPOs. To ease the introduction of Public Wi-Fi, state governments can provide voucher-based funding like the EU for eligible establishments to obtain support for installation or operationalization of Public Wi-Fi.

26. We also recommend that monetary / funding support ought to be differentiated on the basis of specific projects that ensure Public Wi-Fi availability in certain settings. For example, one initiative could install Wi-Fi hotspots in all bus stops and/or state libraries. Rural areas and smaller cities are given more funding given that internet usage and dependence has not risen highly enough for commercial establishments to provide such services as a matter of necessity. A combination of need and policy-based criteria can be employed to determine which establishments or institutions ought to be prioritised. Besides footfall, policy incentives such as education can also be considered. Libraries that have well functioning Wi-Fi systems may be used better than those that do not. Funding can be provided through a mix of grants, loans, grant-loan combinations, voucher-based funding, or subsidies from the Digital Bharat Nidhi.[8]

27. Part of this funding should be specifically used for strengthening backhaul infrastructure till the last-mile of connectivity required in both rural and urban areas. State governments, city-level governments, district administrations, should introduce projects that strengthen street-level fiberisation, with a preliminary focus on public institutions and high footfall areas.

28. Public Wi-Fi systems and networks across the world are construed as less secure than mobile data or private broadband connections. A baseline set of technical and security standards should be set, insofar as they are technically feasible with Public Wi-Fi provisioning. Websites that concern financial, medical, or other sensitive personal data should be expected to alert its users that they are on a public network that is less secure than mobile data.

29. To ease right of way issues, local bodies play a key role in providing faster permissions, streamlining local approvals, finding 'priority' locations that will strategically enhance use of Public Wi-Fi. Local bodies can also provide access to municipal infrastructure like street lights, bus shelters, public buildings, parks, and street furniture. They can also assist in fiberisation of street-level infrastructure and coordination with other civic works to limit disruption to a specific period of time.

30. We recommend that in addition to the funding and facilitative roles of government, State governments or their entities ought not to function as PDOAs. PDOAs provide essential backend services from authorization, accounting, security, network management, and settlement. It is critical that the PDOAs are technically and operationally secure and privacy-respecting, given that they aggregate much of the data that passes through the Public Wi-Fi networks. The state governments cannot function as PDOAs while ensuring the effective implementation of regulatory standards. The state governments ought to function independently from PDOAs. The governments at the Center and the states should ensure that PDOAs provide Wi-Fi that conforms to the necessary regulatory standards.

[8] Telecommunications Act, 2023, ss 24-26.

31. To enhance trust in Public Wi-Fi, PDOs and PDOAs that are conforming to regulatory standards can be given a certificate such as "Friendly Wi-Fi" for ease of identification by the public. Wi-Fi operators whose public Wi-Fi systems strictly meet a certain threshold can be given these uniquely identifiable certificates. Local bodies can also hold awareness sessions that are short and digestible for the public, focusing on access and the most key safety rules. As knowledge around use of Public Wi-Fi systems develops, these awareness sessions could be used to include more aspects.

32. While we recommend that Public Wi-Fis are free or follow a freemium model where only longer usage is chargeable, the revenue stream for ISPs from mobile data and broadband may not reduce to a nullity. In fact, while overall requirement for GBs per month may reduce, mobile data and broadband connection as a whole may not become redundant. Such a perspective must not inform the revenue and monetisation model adopted for Public Wi-Fis. One possibility could be that commercial establishments functioning as PDOs can show costs of Public Wi-Fi operationalisation as part of their CSR initiatives.

33. For the purpose of incentivising the proliferation of fixed line broadband networks, providing direct or indirect incentives to the licensees can lead to several issues, misappropriation of revenues being the most prominent among them.[9] Indirect incentives fail to guarantee that ISP's would invest the increased monies into expanding the user base, especially in rural and far flung areas. This is because direct or indirect incentives provide licensees with significant amounts of discretionary power, as the very nature of direct or indirect incentives allows licenses to choose how to deploy increased resources. It would not be unreasonable to expect ISPs and telecom companies to channelise the surplus revenues to clearing their outstanding AGR dues rather than investing on expanding the user base. As an alternative, we see direct performance linked incentives as a more effective incentive mechanism. There is evidence based merit in opting for post facto incentives based on the growth of the user base as the indisputable metric to determine the benefits of direct benefits. Direct incentives provide a concrete pathway towards increasing the user base. Direct incentives, if linked to investment, also provide a good boost to capital expenditure in the sector, thus enabling the development of infrastructure in under-serviced areas.

34. To summarize, our recommendations are as follows:

    a. The government can explore self-deployment in public institutions like schools, libraries, parks, offices that are administered by the government;

    b. More targeted interventions in private institutions where installing Public Wi-Fi can enhance coverage. This could be by direct funding of the installation of backhaul infrastructure while the operational costs are covered by the commercial establishments / DPOs. To ease the introduction of Public Wi-Fi, state governments

[9] Yashaswini, On the need for citizen oriented growth in the telecom sector, (IFF, 14 June 2021), https://internetfreedom.in/on-the-need-for-citizen-oriented-growth-in-the-telecom-sector/.

can provide voucher-based funding for eligible establishments to obtain support for installation or operationalization of Public Wi-Fi.

c. Monetary / funding support ought to be differentiated on the basis of specific projects that ensure Public Wi-Fi availability in certain settings. A combination of need and policy-based criteria can be employed to determine which establishments or institutions ought to be prioritised. Besides footfall, policy incentives such as education can also be considered. Part of this funding should be specifically used for strengthening backhaul infrastructure till the last-mile of connectivity required in both rural and urban areas.

d. State governments, city-level governments, district administrations, should introduce projects that strengthen street-level fiberisation, with a preliminary focus on public institutions and high footfall areas.

e. A baseline set of technical and security standards should be set, insofar as they are technically feasible with Public Wi-Fi provisioning.

f. State governments or their entities ought not to function as PDOAs. The state governments ought to function independently from PDOAs. The governments at the Center and the states should ensure that PDOAs provide Wi-Fi that conforms to the necessary regulatory standards.

g. To ease right of way issues, local bodies play a key role in providing faster permissions, streamlining local approvals, finding 'priority' locations that will strategically enhance use of Public Wi-Fi. Local bodies can also provide access to municipal infrastructure like street lights, bus shelters, public buildings, parks, and street furniture. They can also assist in fiberisation of street-level infrastructure and coordination with other civic works to limit disruption to a specific period of time.

h. To enhance trust in Public Wi-Fi, PDOs and PDOAs that are conforming to regulatory standards can be given a certificate such as "Friendly Wi-Fi" for ease of identification by the public.

i. Public Wi-Fis must be free or follow a freemium model where only longer usage is chargeable. However, the revenue/monetisation model should not be built on the false basis that revenue stream for ISPs from mobile data and broadband may not reduce to a nullity. International experience suggests that while overall requirement for GBs per month may reduce, mobile data and broadband connection as a whole may not become redundant.