INDIAN GOVERNANCE AND POLICY PROJECT

IGAP Comments

Draft National Telecom Policy, 2025

Authored by
Dedipyaman Shukla

With inputs from
Shachi Solanki
and Jhanvi Anam

Preliminary Comments

At the outset, we welcome the opportunity provided by the Department of Telecommunications ***(DoT)*** to submit feedback on the Draft National Telecom Policy, 2025 ***(Draft NTP)***. The incorporation of a diversity of inputs from stakeholders across India's ICT and telecommunication ecosystem is integral to realising the policy's broader goals of economic development, social empowerment, and technological innovation.

As of June 2025, India is home to about 1.08 billion active mobile subscribers, with an overall tele-density of 86.09 percent.[1] The rapid growth of mobile-based services has enabled India to build one of the largest digital economies in the world, which is estimated to comprise 13.42 percent of India's national income in 2024-25.[2] To preserve the robust growth and resilience of the digital economy, the Draft NTP will need to focus on enhancing network infrastructure, ensuring equitable access to high-speed connectivity across urban and rural areas, strengthening cybersecurity frameworks, and promoting innovation-friendly regulatory policies that can accommodate emerging technologies while safeguarding users.

The following comments, submitted on behalf of the Indian Governance and Policy Project ***(IGAP)***, a premier think-tank dedicated to enhancing domestic governance frameworks, aim to address the competing concerns of national security, increased sectoral innovation, and consumer interest, in the context of India's evolving digital governance framework.

Managing Privacy Implications from the Collection of Biometric User Data

The Draft NTP seeks to establish a biometric-based identification for all telecom users to ensure privacy and protection. Rather than enhancing privacy, the proposal, in practice, may help improve the monitoring of the misuse of telecom resources. However, this increased data processing may also result in harms towards Indian citizens. Biometric data, by its nature, relates to behavioural or physiological data-points which are unique to an individual. Such data collected through automated means, in relation to telecom users, would come under the ambit of 'personal data' within the Digital Personal Data Protection Act, 2023 ***(DPDP Act)***.[3] The processing of biometric data is widely understood to result in higher privacy risks for users as compared to other forms of personal data.[4] Breach of such information may result in unauthorized accessed to sensitive resources, identity theft, and even fraud.[5]

A considerable degree of cyber-security measures would need to be implemented by data fiduciaries in relation to such data. Further, its collection and processing would need to follow the principles of data minimization, as incorporated in the new data protection law. Nonetheless, it should be noted that the monitoring of information security practices and cyber-incident reporting compliances among Indian data fiduciaries is not adequate.[6] This may be further hampered by resource constraints post the implementation of the DPDP Act.[7]

As a consequence, the biometric-based identification of all telecom users may place more than 1 billion subscribers at an enhanced risk of data breach and consequent harms.

Additionally, concerns regarding the acquisition of telecom services by users with forged identification were previously noted by the Telecom Regulatory Authority of India ***(TRAI)***. After detailed consultations on the subject, the authority recommended the use of Aadhaar-based e-KYC as a beneficial solution for all stakeholders.[8] At present, the Draft NTP neither explains how biometric authentication directly enables user privacy, nor does it demonstrate why less intrusive methods such as e-KYC with informed consent, multi-factor authentication, etc. are insufficient to meet the same goal.

Recommendation

The policy should reconsider the use of biometric identification as a privacy-enabling tool. Unless it can be demonstrated that this measure is not overly restrictive, technically justified, and accompanied by enforceable data security standards, alternative authentication mechanisms, such as e-KYC may be pursued.

Clarifying the Blocking of Access to Internet Resources via Telecommunication Services

The Draft NTP proposes that a 'policy and regulatory framework for blocking rogue IPs/URLs/Applications and its implementation in TSP/ISP network' be defined under 'Mission 4: Secure and Trusted Network'. This proposal has intersections with the established legal authority under Section 69A of the Information Technology Act, 2000, intended for the internet and content-layer blocking. Section 69A empowers the Central Government to direct blocking of access to information through any computer resource, and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 lay down the requisite procedure for the same. Therefore, the Draft NTP proposal may carry the potential for DoT to create new or parallel regulations, rather than complementing existing ones. Further, executive actions under the DoT must acknowledge the mandate under the Government of India (Allocation of Business) Rules 1961, which places all policy matters relating to the 'internet' (apart from the licensing of ISPs) under MEITY. Accordingly, the scope of this proposal under the Draft NTP may be further clarified or narrowed, as relating to the implementation mechanics, such as network-side capabilities to comply with valid blocking orders under Section 69A of the Information Technology Act, 2000.

Recommendation

To prevent legal and institutional fragmentation, the Draft NTP should clarify that DoT will act in coordination with MEITY, and under the established Information Technology Act, 2000 for blocking of internet resources. The language should be revised to reflect a 'support role' for DoT, focusing on technical enforcement (for example, implementation protocols for TSPs/ISPs), rather than policy formulation. This would preserve the constitutional and statutory safeguards under the IT Act, ensure legal consistency, and avoid duplication of regulatory powers.

Addressing Public Wi-Fi Cybersecurity Risks

The Draft NTP further seeks to promote public Wi-Fi access through the PM-WANI framework. However, adequate user privacy awareness measures have yet to be incorporated within the public Wi-Fi policy design. Without strong safeguards, public Wi-Fi networks may risk becoming vulnerable to hacks and breaches,[9] particularly when authentication mechanisms are linked to personal identifiers such as mobile numbers. Additionally, many users, particularly in rural and first-time internet adoption contexts, may not understand how easily unencrypted traffic on public Wi-Fi can be monitored or manipulated, or how to use basic protections like VPNs, HTTPS verification, and device-level firewalls. Without targeted digital literacy campaigns, PM-WANI's mission risks being undermined by privacy breaches and cyber fraud, potentially eroding public trust in the scheme and deterring its long-term adoption. Crucially, the proposal must include a mandate to build robust cybersecurity awareness to support these networks. This is significant, especially given the volume of sensitive use cases such as banking, education, healthcare, etc. that increasingly rely on wireless connectivity.

Recommendation

The policy must incorporate a robust privacy by design philosophy, alongside enhanced user awareness programs on the risks of public Wi-Fi based internet access, in conjunction with other relevant government stakeholders such as MEITY. This includes ensuring transparency in terms of data retention, limiting third-party access, and aligning the policy with the soon to be enforced Digital Personal Data Protection Act, 2023.

4

Realizing Universal and Meaningful Connectivity Across India

Under Mission 1, the policy sets an ambitious target of achieving 100% population coverage with 4G and 90% with 5G by 2030. This vision aligns with global digital development frameworks, including the UN & International Telecommunication Union ***(ITU)***'s Universal Meaningful Connectivity targets.[10] While the mission to empower all citizens with state-of-the-art telecom facilities is commendable, India's remote and tribal regions continue to face enduring multivariate barriers to access including difficult terrain, low monetization potential, effects of Left-Wing Extremism, and State-level Right-of-Way ***(RoW)*** delays.[11] As of 2025, 2,595 villages belonging to Particularly Vulnerable Tribal Groups across 15 states were identified as in need of mobile tower installations.[12]

Recommendation

To ensure that the universal 4G and 5G coverage target translates into effective implementation, the policy must formulate district-level or state-wise milestones for 4G and 5G rollout in order to operationalize the mission. Most critically, the policy should also outline the need for robust and transparent enforcement frameworks, with clear financing pathways. Without these, the targets risk remaining aspirational especially in low 'Average Revenue Per User' rural areas, where private sector participation is constrained by limited commercial viability.

5

Address Gender-Gap in Device Accessibility

Within the Draft NTP, the inclusion of device accessibility is a welcome step however, there is a lack of recognition of a persistent gender gap in mobile internet access. In India, it is estimated that women are 40% less likely than men to either own a mobile phone or use mobile internet.[13] This divide has direct consequences for women's access to essential services such as education, healthcare, financial inclusion, and digital livelihoods. It also hinders their ability to benefit from government schemes increasingly delivered via digital platforms. Crucially, this gap is not just a user side concern and may also distort the datasets on which emerging technologies like AI may be trained.[14] This creates downstream harms including biased AI systems, limited vernacular content, and the reduced relevance of digital services for the very groups the Digital India mission aims to include.

Recommendation

To address this, the Draft NTP must explicitly recognise the need for targeted initiatives for enhancing user-side device accessibility across the gender-divide. The DoT may consider collaboration with MEITY and the Ministry of Women and Child Development to integrate device access with digital literacy and safety programs, and promote data-driven research on gender-based device access and internet usage.

Co-ordinated Approach to Telecom Innovation

The innovation mission in the Draft NTP outlines an ambitious vision to position India as a global innovation hub in emerging telecom technologies including 5G/6G, AI, IoT, and quantum communications. It proposes a broad set of strategies covering R&D funding, spectrum liberalization, IPR generation and start-up support. Furthermore, the policy's emphasis on strengthening telecom infrastructure is particularly important not only as a driver of innovation in telecom itself, but also for accelerating AI adoption, as reliable and high-speed connectivity is essential for large-scale data processing, model deployment, and last-mile delivery of AI services. Conversely, the integration of AI into telecom networks enhances their resilience, adaptability, and efficiency. These technologies intersect with domains under the purview of multiple union ministries (electronics and IT, science and technology, skill development, space, defence, and higher education), as well as the flagship 'India AI Mission', which seeks to promote socially impactful AI projects.

Innovation in these interdisciplinary sectors depends on coordinated policy, funding, and synergized regulatory frameworks. Without structured collaboration, shared infrastructure, and joint innovation roadmaps, the efforts under the DoT risk duplication, fragmented implementation, and reduced global competitiveness. Reference to a cross-sectoral governance mechanism, such as the Prime Minister's

Science, Technology and Innovation Advisory Council[15] ***(PM-STIAC)***, is essential to ensure that India's telecom innovation leadership is embedded within the broader national ecosystem for deep-tech innovation and digital transformation.

Recommendation

The Draft NTP may embed joint roadmaps, shared infrastructure, and unified funding mechanisms to ensure telecom innovations advance within a coherent national strategy for all deep-tech.

Endnotes

1. TRAI, Press Release No. 64/2025, available at <https://www.trai.gov.in/sites/default/files/2025-07/PR_No.64of2025_0.pdf>

2. MEITY, Estimation and Measure of India's Digital Economy, January 2025, (p.13), available at <https://www.meity.gov.in/static/uploads/2025/01/5ff397f9e8152d5562ed4cef1a6b767b.pdf>

3. Digital Personal Data Protection Act, 2023, Section 2(t) defines personal data as any data about an individual who is identifiable by or in relation to such data.

4. Dutch DPA, Rules for the use of biometrics, available at <https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/rules-for-the-use-of-biometrics#privacy-risks-associated-with-biometric-data>

5. Wang M, Qin Y, Liu J, Li W. Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks. Humanit Soc Sci Commun. 2023;10(1):216. doi: 10.1057/s41599-023-01673-3. Epub 2023 May 8. PMID: 37192941; PMCID: PMC10166458.

6. Maheshwari et al., Anticipating Compliance with the Digital Personal Data Protection Act, 2023 on Data Breaches in India, Indian Governance and Policy Project Report, November 2023, available at <https://www.igap.in/anticipating-compliance-with-the-digital-personal-data-protection-act-2023-on-data-breaches-in-india-2/>

7. Ibid

8. TRAI Recommendations, January 2017, available at <https://www.trai.gov.in/sites/default/files/2024-11/E_KYC_services_Rec_20_01_2017.pdf>

9. Indian Express, Are you safe on public Wi-Fi? What you need to know now, May 2 2025, available at <https://indianexpress.com/article/technology/tech-news-technology/are-you-safe-on-public-wi-fi-what-you-need-to-know-now-9681879/>

10. ITU Press Release, New UN targets chart path to universal meaningful connectivity, April 2022, available at <https://www.itu.int/en/mediacentre/Pages/PR-2022-04-19-UN-targets-universal-meaningful-connectivity.aspx>

11. EY Report, Gati Shakti, September 2022, available at <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/insights/telecommunications/documents/ey-dipa-repoert-gati-shakti-paving-the-way-for-accelerated-digital-infrastructure-rollout-in-india.pdf?>

12. Ministry of Communications Press Release, 6 February 2025, available at <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2100354>

13. Accelerating Indian Women's Use of Mobile Phones through Low-Cost Training in Digital Skills Improves Their Mental Health, Yale Economic Center, available at <https://ie.yale.edu/sites/default/files/2024-03/GMA%20Policy%20Brief.pdf>

14. Bolukbasi et al., Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings, 30th Conference on Neural Information Processing Systems (NIPS 2016), available at <https://proceedings.neurips.cc/paper_files/paper/2016/file/a486cd07e4ac3d270571622f4f316ec5-Paper.pdf>

15. About PM-STIAC, Available at <https://www.psa.gov.in/pm-stiac>

INDIAN GOVERNANCE AND POLICY PROJECT

The Indian Governance And Policy Project **(IGAP)** is an emerging think tank focused on driving growth, innovation, and development in India's digital landscape. Specializing in areas like AI, Data Protection, FinTech, and Sustainability, **IGAP** promotes evidence-based policymaking through interdisciplinary research. By working closely with industry bodies in the digital sector, **IGAP** provides valuable insights and supports informed decision-making. Core work streams include policy monitoring, knowledge dissemination, capacity development, dialogue and collaboration.

For more details visit: www.igap.in

relations@igap.in | igap.in