Prashant Vilas Kumbhar

Digital Public Infrastructure over Digital Commons:

India's Governance Choice and Its Trade-offs for Inclusion, State Power, and Data Sovereignty

---

In recent years, India has increasingly been **positioned within policy discourse** as an example of digital public infrastructure (DPI), offering a state-led alternative to intermediary platform capitalism. However, this raises a core policy dilemma: while DPI can deliver scale and inclusion, it also restructures power, participation, and sovereignty in ways that differ fundamentally from digital commons-based models.

1. Core Policy Question

Why has India prioritised digital public infrastructure over digital commons as one of its major modes of digital governance, and what are the trade-offs of this choice for digital inclusion, state power, and data sovereignty?

2. Analytical Framing

Large-scale DPI systems like Aadhaar, the Unified Payments Interface (UPI), and, more recently, the Open Network for Digital Commerce (ONDC) are part of India's digital governance strategy. In policy discourse, these systems are frequently referred to as 'public goods' or 'digital public commons' interchangeably. However, if assessed against the course definition of digital commons non-rival resources governed through shared arrangements that allow free use, modification, and redistribution, India's DPI follows a different logic. The state built foundational digital infrastructure (identity, payments, data rails), while private actors innovated at the application and service layer (RIS, 2025).

India has prioritised a centrally coordinated infrastructure that emphasises scale due to its high and diverse population, interoperability due to administrative fragmentation and uneven state capacity, and central administrative control due to limited provincial resources. These conditions made DPI a more feasible and politically legitimate model than digital commons.

3. Preference for Digital Public Infrastructure

Digital commons require sustained collective governance, maintenance, high digital literacy, and institutional trust across diverse actors (Dulong de Rosnay & Stalder, 2020). In the Indian context, such conditions were weak. The state, therefore, prioritised DPI as a way to achieve rapid scale while maintaining administrative legibility. For instance, Aadhaar was intended to establish a single identity layer that could be required for all welfare programs. As O'Neil et al. (2021) note, open-source and commons-based production require mechanisms to balance power asymmetries. India opted for regulatory authority and institutional oversight to manage those asymmetries.

Additionally, the absence of a strong domestic digital platform initially created incentives to build state-led alternatives. Digital commons rely on transnational trust and shared governance arrangements

that limit unilateral control (Dulong de Rosnay & Stalder, 2020). However, geopolitical tensions can erode the political legitimacy of such arrangements. India's 2020 ban on Chinese mobile applications on grounds of data security and threats to sovereignty illustrates exclusion and domestic control over openness (Ministry of Electronics & IT, 2020). While not a rejection of digital commons per se, such measures reduce the political space for commons-based governance and help explain India's preference for centrally governed digital public infrastructure in sensitive domains. However, India's preference for digital public infrastructure can not be interpreted as an absence of digital commons. This does not imply an absence of digital commons: India's BOSS Linux, built on Debian, is a suitable example of digital commons.

4. Trade-offs for Digital Inclusion

India's DPI has improved access in quantifiable ways. Aadhaar-linked welfare delivery reduced duplication, while UPI expanded digital payments far beyond metropolitan centres. DPI has been successful in reducing transaction costs and expanding basic services from the perspective of inclusion. In March 2025, UPI processed more than 12.1 billion transactions, solidifying its position as the most popular digital payment system globally (Coin Law, 2025). To note, over 55% of rural India now uses UPI for digital payments. However, this inclusion is conditional rather than participatory. In centrally managed systems, access is contingent upon enrollment, compliance, and authentication. DPI governance can not be significantly influenced by users, and innovations can not arise through forking. In one widely reported 2017 case, an 11-year-old girl reportedly died after her family's ration food card was cancelled for not being Aadhaar-linked, an incident linked to exclusion (NDTV, 2017). This causality remains contested, such cases illustrate the coercive effects of centralised data infrastructures without shared access.

5. Trade-offs for State Power

DPI has expanded the Indian state's capacity for surveillance and informational capacity (RIS, 2023). Through Aadhaar, the state gained unprecedented visibility into beneficiary populations. Through UPI, it acquired oversight over payment flows previously mediated by private banks. Nevertheless, this centralises risk through governance failures, data breaches, or exclusion errors, which have system-wide consequences. In 2020, cybersecurity researchers reported that a misconfigured cloud storage bucket linked to a BHIM-related onboarding website (Part of UPI) exposed personal and financial data of approximately 7.26 million users, including identity documents and biometric information. While NPCI denied a breach of the core BHIM system, independent analysis confirmed it (Vijayan, 2020). While this does not imply pervasive surveillance, it increases asymmetries between the state and citizens by centralising visibility and decision-making authority within unshared digital systems.

6. Trade-offs for Data Sovereignty

India articulates data sovereignty primarily as a public interest concern tied to accountability and national autonomy. The Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India (2017)* constitutionally constrained state collection and use of personal data by subjecting such actions to legality, necessity, and proportionality requirements. The Digital Personal Data Protection Act, 2023 (DPDP) requires UPI to implement security standards, breach notification, and clear

consent mechanisms (Lawrbit, 2025). Yet, DPI complicates sovereignty. Interoperability risks sliding into digital protectionism. It raises concerns about the potential weaponisation of data. In this sense, sovereignty achieved through infrastructure differs qualitatively from sovereignty grounded in commoning. Pollock (2016) cautions that governments benefit most from openness when they invest in shared governance. India's DPI illustrates this tension: sovereignty is strengthened institutionally, but at the expense of transnational cooperation and commons-based innovation.

7. Conclusion

To conclude, India's preference for digital public infrastructure over digital commons indicates pragmatic responses to scale, capacity, and political economy constraints. This choice has delivered tangible gains in inclusion and state capability, while limiting dependence on shared global platforms. However, it also has an opportunity cost with a narrowed space for shared governance, participatory control, and commoning practices. The significance of this choice lies not in whether DPI succeeds or fails, but in how it redefines the meaning of digital sovereignty. Seen in this light, India's experience suggests that where scale and state capacity dominate policy imperatives, commons-based governance becomes residual rather than foundational.

References (APA)

1. O'Neil, M., Cai, X., Muselli, L., Pailler, F., & Zacchiroli, S. (2021). *The co-production of open source software by volunteers and big tech firms*. Digital Commons Policy Council, University of Canberra. https://dcpc.info/publications/the-coproduction-of-open-source-software-by-volunteers-and-big-tech-firms/
2. Pollock, R. (2016). Why open source software matters for the government. https://rufuspollock.com/open-source-software-and-government/
3. Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. https://indiankanoon.org/doc/127517806/
4. Lawrbit. (2025). *Digital Personal Data Protection Rules, 2025: Key highlights and implications*. https://www.lawrbit.com/article/digital-personal-data-protection-rules-2025/
5. Vijayan. Dark Reading. (2023). *Data on Indian mobile payments apps reportedly exposed via open S3 bucket*. https://www.darkreading.com/cyberattacks-data-breaches/data-on-indian-mobile-payments-app-reportedly-exposed-via-open-s3-bucket
6. NDTV. (2017, September 28). *"No Aadhaar, no food": 11-year-old girl died begging for rice, says Jharkhand family*.
7. https://www.ndtv.com/india-news/no-aadhaar-no-food-11-year-old-girl-died-begging-for-rice-says-jharkhand-family-1763863
8. Dulong de Rosnay, M., & Stalder, F. (2020). Digital commons. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1530
9. Press Information Bureau, Government of India. (n.d.). *Press release*. https://www.pib.gov.in/PressReleseDetailm.aspx