



UPSC &amp; STATE PCS CURRENT AFFAIRS · UJIYARI.COM

**EDITORIAL ANALYSIS**

# India Stack's Global Ambition – DPI as Sovereignty or New Dependency?

INDIAN EXPRESS

22 February 2026

## SUBJECTS COVERED

SCIENCE &amp; TECH

IR

POLITY

## GS PAPERS

GS2

GS3

## CURATED &amp; WRITTEN BY

**Bharat Choudhary**

UPSC Educator &amp; Content Creator •

[linkedin.com/in/epicbharat](https://www.linkedin.com/in/epicbharat)

Free UPSC &amp; State PCS Resources

[ujiyari.com](http://ujiyari.com)

# India Stack's Global Ambition — DPI as Sovereignty or New Dependency?

 The Indian Express

22 February 2026

GS2

GS3



The Indian Express

MAINS RELEVANCE:

GS Paper 2

GS Paper 3



## INTERVIEW ANGLE

*"India promotes its Digital Public Infrastructure as a sovereignty-preserving alternative to corporate platform colonialism. But DPI built on Aadhaar raises serious surveillance and exclusion concerns within India itself. Can India export a model it has not fully resolved domestically? And is DPI truly about development or about geopolitical positioning?"*

India Stack is genuinely impressive. A biometric identity system covering 1.38 billion people. A payments network processing 14 billion transactions a month at near-zero cost. Digital document infrastructure that has eliminated billions of rupees in government benefit leakage. These are real achievements — ones that took decades of patient institution-building and political will.

The question raised by India Stack Global is whether what worked in India — built over 15 years in a specific political, regulatory, and social context — can or should be exported as a development solution to other countries.

## WHAT INDIA STACK DID RIGHT

The core insight behind India Stack was **interoperability as public good**. Rather than letting private companies (banks, telecom providers, retailers) build isolated digital infrastructure that locks users in, India built **open, government-operated infrastructure that any private player can plug into**.

This is architecturally important. When UPI is the payments rails, no single company owns the network. Paytm, PhonePe, Google Pay, and BHIM all operate on the same infrastructure — competing on service, not on infrastructure ownership. The network effects accrue to the system, not to any one player. Compare this with WeChat Pay or Alipay in China, where two companies effectively own China's digital payment system.

The **Account Aggregator** framework extends this principle to data. Citizens — not banks or fintechs — control their financial data. When a citizen wants a small business loan, they can instantly share (and revoke access to) their bank statements with a lender. This is consent-based data sharing at scale — a genuine innovation in financial services architecture.

## THE AADHAAR PROBLEM — UNRESOLVED TENSIONS

But India Stack's foundation — Aadhaar — has unresolved tensions that India must be transparent about when promoting it globally.

**Exclusion.** The shift to Aadhaar-linked benefit delivery has caused documented exclusion. When the elderly, homeless, or migrant workers cannot authenticate their fingerprints (due to age, manual labour, or lack of mobile connectivity), they are denied food rations, pensions, and welfare. **Starvation deaths** in Jharkhand and other states were linked to failed Aadhaar authentication. The Supreme Court's Puttaswamy judgment (2018) upheld Aadhaar's constitutional validity but restricted mandatory linking to government benefits — precisely because of exclusion risks.

**Surveillance.** Aadhaar's centralized biometric database — run by UIDAI (Unique Identification Authority of India) — creates the technical infrastructure for mass surveillance. The government maintains it does not link Aadhaar to CCTV, social media, or political activity. But the infrastructure could be repurposed. For a developing country considering adoption, the government in power ten years from now may have different intentions than today's.

**Mission creep.** Despite Supreme Court restrictions, Aadhaar linking has expanded far beyond its originally stated purpose of subsidy delivery — to SIM cards, bank accounts, company registrations, and more. Each expansion, justified individually, creates a more comprehensive data profile of citizens.

## WHAT OTHER COUNTRIES SHOULD CONSIDER

For a Sierra Leone or Papua New Guinea considering India Stack adoption, the trade-offs are not the same as they were for India. India had:

- A mature democracy with judicial oversight (Supreme Court ultimately restricted Aadhaar's scope)
- Civil society organisations capable of litigation and advocacy
- A federal structure creating multiple check points
- Pre-existing administrative capacity

Most of India Stack's partner countries have weaker institutional guardrails. A government digital identity system without robust courts to challenge misuse, without civil society to document exclusion, and without free press to amplify abuse is a very different proposition.

## THE GEOPOLITICAL DIMENSION

India promotes DPI as an alternative to “platform colonialism” — Western tech giants owning developing world digital infrastructure. The framing is correct. Facebook's Free Basics programme (attempting to position Facebook as the internet for billions in developing countries) was rightly rejected.

But India Stack Global also has a geopolitical calculation: countries that adopt India’s DPI become, to varying degrees, aligned with India’s technology standards, dependent on Indian technical assistance, and linked to India’s diplomatic network. This is a form of soft power — no different from China’s Digital Silk Road or the West’s promotion of democracy-compatible technology frameworks.

This is not inherently wrong — soft power is legitimate statecraft. But it should be named honestly. DPI export is partly development cooperation and partly India building a sphere of digital influence.

The honest case for India Stack Global is: India has built something that genuinely works at scale for financial inclusion, and the world’s poorest countries deserve access to that architecture. The guardrails that India got wrong — exclusion, surveillance risks — can be designed out from the start in new implementations, with stronger consent architecture and mandatory offline fallbacks. If India can make that case transparently, the global DPI project is worth supporting.

### UPSC RELEVANCE

India Stack, Aadhaar (1.38B enrolled), UIDAI, UPI (14B txn/month), Account Aggregator, DPDP Act 2023, Puttaswamy judgment (2018), JAM Trinity, India Stack Global partner countries.

### MAINS GS-2:

Digital governance; surveillance vs. inclusion trade-off; Supreme Court and fundamental rights.

### GS-3:

Digital public infrastructure; financial inclusion; data governance; India’s tech diplomacy.

### INTERVIEW:

“The Supreme Court in the Puttaswamy case said privacy is a fundamental right. Does Aadhaar violate this right despite the Court’s validation of the scheme?”

★ **FACTS CORNER — KNOWLEDGEPEDIA**

**AADHAAR LEGAL HISTORY:**

Justice K.S. Puttaswamy vs. Union of India (2017): **Privacy is a fundamental right** (9-judge bench)

Puttaswamy (2018): Aadhaar upheld but **mandatory linking to private services struck down**

Allowed: Linking to government benefits (PDS, LPG, MGNREGS)

Struck down: Mandatory linking to bank accounts (for private purposes), SIM cards

UIDAI: Unique Identification Authority of India; operates Aadhaar; under MeitY

**AADHAAR EXCLUSION ISSUES:**

Failed biometric authentication: Elderly, manual labourers, migrants

Jharkhand starvation deaths: Linked to Aadhaar authentication failures in PDS

Offline solution: **Aadhaar Virtual ID** (16-digit temporary ID for authentication without sharing Aadhaar number)

**DPDP ACT 2023:**

Full form: Digital Personal Data Protection Act, 2023

Governs: Collection, processing, storage of personal data including Aadhaar-linked data

Key right: Right to erase data (right to be forgotten)

Data Fiduciary: Any entity processing personal data; must ensure consent

**INDIA STACK GLOBAL — HONEST ASSESSMENT:**

Strengths: Open source, interoperable, proven at scale, zero-cost payments

Risks to watch in export: Exclusion without offline fallbacks, surveillance risk without judicial guardrails, mission creep

Safeguard design: Offline authentication modes, consent architecture, data minimisation principles

Sources: Indian Express, UIDAI, PIB

---

CURATED & WRITTEN BY

# Bharat Choudhary

UPSC Educator & Content Creator

 [linkedin.com/in/epicbharat](https://www.linkedin.com/in/epicbharat)

---

Published on [ujjari.com](http://ujjari.com) · Free UPSC & State PCS Current Affairs