

DPI UNDER SIEGE

Where Scale Creates New Governance Risks

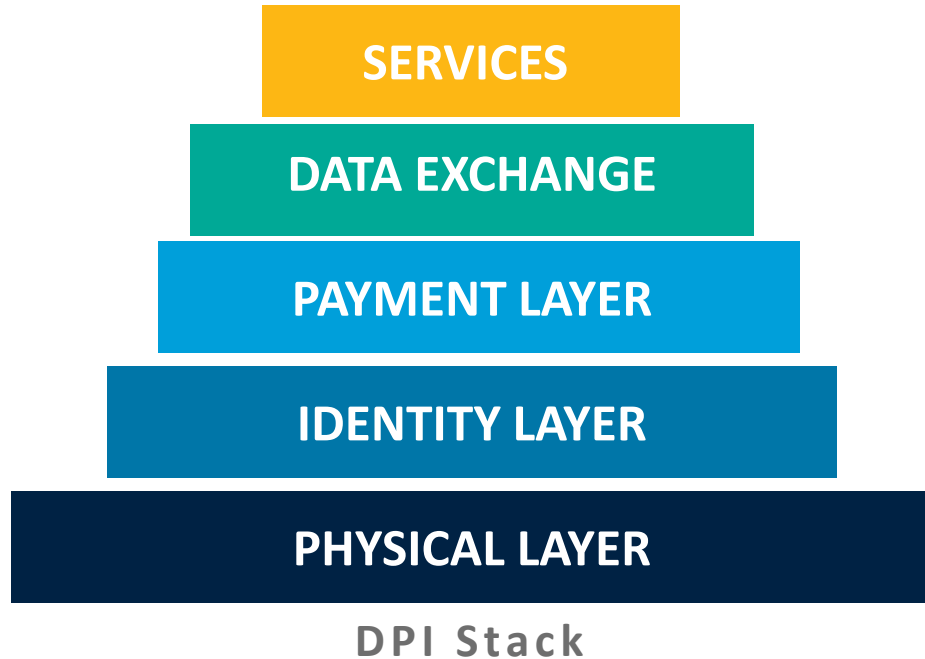
©Tariq Malik | Former Chairman NADRA



**Can DPI concentrate
Power, Risk & Control?**

The Promise of Digital Public Infrastructure

DPI is designed to transform how nations serve their citizens by reusing Digital Assets



Inclusion
Reach unbanked & underserved populations

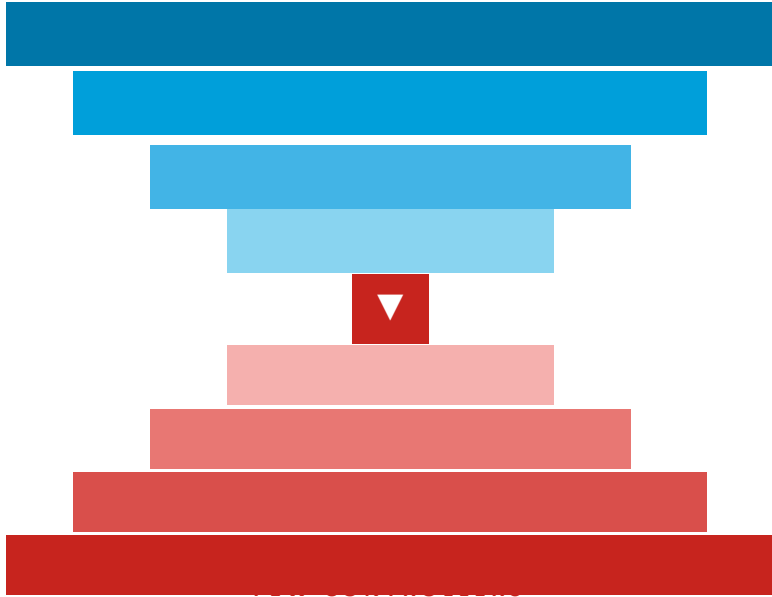
Efficiency
Eliminate friction, reduce costs, speed delivery

Transparency
Auditable, open systems reduce corruption

Scale
Serve hundreds of millions simultaneously

The Hidden Reality

What DPI promises and what it actually concentrates are not the same thing



DPI concentrates: Power

Decisions about access, identity and participation shift to platform operators, not governments, not citizens.

DPI concentrates: Risk

Systemic risk aggregates at the infrastructure layer. A single failure disables millions simultaneously.

DPI concentrates: Control

Jurisdictional sovereignty erodes when critical infrastructure is governed by foreign corporate architecture.

Image generated by AI

CASE STUDIES

DPI in Practice:

When Infrastructure Becomes an Instrument of Control

China

India

Africa

EU / UK

Pakistan

CHINA

DPI as Surveillance Infrastructure?

China's Social Credit System

HOW IT WORKS

Identity Layer

National ID links bank accounts, travel, housing, employment and social media into one surveillance graph.

Behavioural Scoring

[System](#) aggregates legal, financial, and administrative records across agencies

Automated Consequence

Low scores trigger travel bans, and loan refusals.

Real-time Enforcement

Facial recognition is widely deployed in local [enforcement](#) contexts.

BY THE NUMBERS

1.1+ Billions approx.
Aggregated financial, legal, admin records

700M+
CCTV cameras

Tens of Millions
Flights & trains travel restrictions

2014
Social Credit Planning framework issued

▶ **Policy lesson: A unified identity layer with no judicial oversight is a control apparatus.**

INDIA

Aadhaar

The world's largest biometric ID system

DOCUMENTED CONCERNS

2017–19 Welfare Exclusion

Many denied food rations [when biometric readers failed](#). Starvation deaths documented in Jharkhand.

2018 & 2025 System Vulnerabilities

[Tribune investigation](#): Unauthorized access. Partial [breaches](#).

2019 Linkage b/w Identity & Citizenship

Aadhaar linked to National Register of Citizens, fears of [exclusion](#) of vulnerable population from legal ID i

2023 Concerns of Surveillance Expansion

[Aadhaar APIs](#) used by private actors for location tracking without consent or oversight.

THE SCALE

1.43 Billion
Aadhaar unique IDs generated

POLICY PRESCRIPTION

Mandatory offline fallback: No single-gate access to welfare

Independent data regulator: Digital Personal Data Protection Act (DPDPA), 2023

AFRICA

Digital Dependency Under Stress: Shutdowns, Conflict, and Platform Concentration

KENYA M-Pesa & Finance Bill Protests

June 2024: Protests against the Finance Bill escalated into a major national political crisis

Internet slowdowns: [Reports](#) of slowdowns during peak protest hours.

Digital Surveillance: Arrests followed the protests, raising concerns about the role of [digital surveillance](#) and telecom data in public-order

18 months Internet [blackout](#) Tigray

ETHIOPIA & DPI in Conflict Zone

2020–22 Tigray War: Internet and telecoms shut down entirely for 18+ months, [longest](#) documented shutdown.

Banking suspended: ATMs and mobile banking disabled. Civilians unable to access food, medicine

Humanitarian Aid blocked: Aid orgs were unable to verify beneficiaries, distribute aid effectively

UN documented: [Denial of services](#)

100+ African shutdowns (since 2020)

Even High-Capacity Systems Face Governance Gaps

Facial recognition, protest monitoring, and consent manufacturing in liberal democracies

UK Live Facial Recognition

2017–present: Met Police deployed LFR at Notting Hill, football, retail without parliamentary approval.

2019- 81%+ false positives in early South Wales

Police [trials](#)

2024 expansion: UK has expanded LFR in policing while statutory framework is incomplete

EU Chat Control Regulation

2022–2024: EU proposed mass scanning of approved private messages to detect CSAM, including encrypted chats (currently heavily contested)

Surveillance by design? UN Special Rapporteur [warned](#) it would create generalised surveillance infrastructure.

UK/Canada Financial Deplatforming

2023 NatWest/Farage: Bank closed account citing 'values', financial DPI used for political exclusion.

Canada 2022: Emergencies Act [froze](#) accounts of 200+ protesters, reversed after 10 days.

Policy gap: No democratic framework governs financial DPI as sanction against citizens.

EU eIDAS 2.0 Digital Wallets

eIDAS 2.0 (2024): EU offering digital ID wallets to all citizens –potentially 450M citizens across member states.

Article 45 risk: Browser root cert provision would have allowed state MITM of encrypted traffic, removed after backlash.

▶ Liberal democracies face same risks but judicial and press accountability can still push back.

Pakistan's NADRA: DPI's Dual Edge

The same system that delivered inclusion at scale illustrates how scale without governance safeguards can create institutional vulnerability.

WHAT DPI DELIVERED (2021–2023)

97%

Adult ID coverage

Near-universal registration, gender gap ↓

10.6M

ASAAN bank accounts

KYC drove financial inclusion; 40% owned by women

\$7B

Roshan Digital Account inflows

NADRA KYC powered overseas Pakistani remittances (2021–23)

53,000

Property cases resolved

Digital succession certificates cut court backlogs by 30%

15M

Flood-affected families

BISP enabled rapid disaster relief targeting

THE POLITICAL BLOWBACK

4M living citizens wrongly marked 'deceased' in electoral rolls.-later rectified

**ELECTION
INTEGRITY**

All identified potential taxpayers. Project was delayed & outsourced to private firm

**TAX REFORMS
DELAYED**

Consent based data sharing was blocked by banks and state agencies fearing accountability.

**PRIVACY
UNDERMINED**

Leadership shifts raise questions about institutional independence

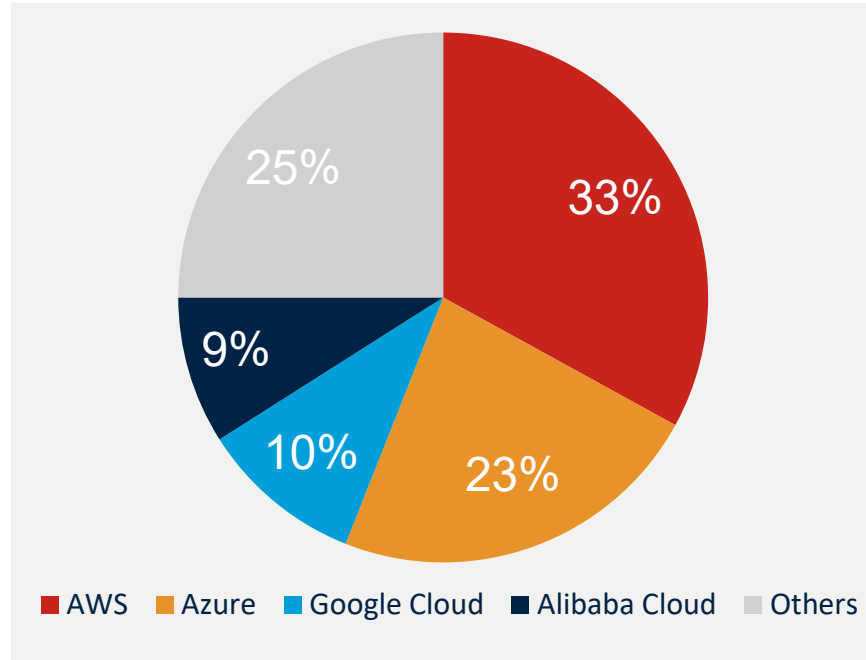
**INSTITUTIONAL
CAPTURE**

DPI that threatens rent-seeking will face institutional capture

Scale and governance must advance together

Cloud Dependency Risk

Most DPI depends on a small number of infrastructure providers, in foreign jurisdictions



33%

AWS

Market share; single largest DPI dependency

56%

AWS + Azure

controls majority of national DPI backends

75%

Top 3 Providers

Host the majority of global DPI systems

Source: Synergy Research (2024); Gartner (2023); OECD (2024)

► **US CLOUD Act (2018) allows US agencies to compel disclosure of citizen data held abroad by American cloud providers.**

The Sovereignty Trap

How DPI dependency creates layered vulnerabilities, each cascading upward

GOVERNMENT SERVICES

Citizens depend on digital services for welfare, ID, banking

DIGITAL PUBLIC INFRASTRUCTURE

Identity, payment, data-exchange (the middle layer)

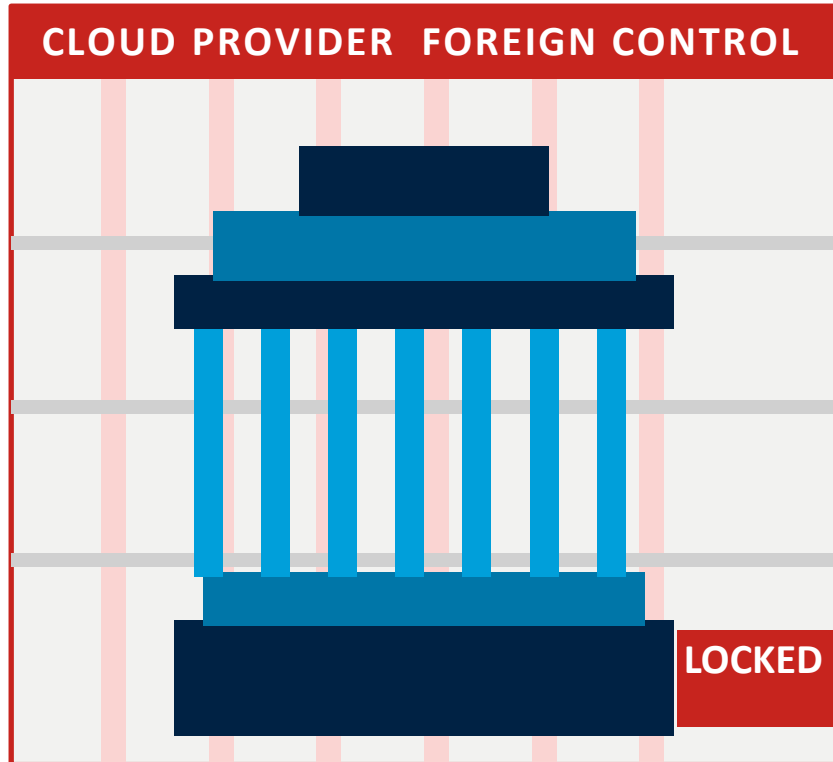
CLOUD PROVIDER

AWS / Azure / GCP: external control, foreign jurisdiction, CLOUD Act risk

- ▶ **Failure at any layer cascades upward: cloud outage = government paralysis.**
External control, foreign jurisdiction, CLOUD Act exposure

Sovereignty Risk

who controls the architecture can shape the state's operational autonomy



Control shifts:

STATE

Elected government holds sovereign mandate

PLATFORM

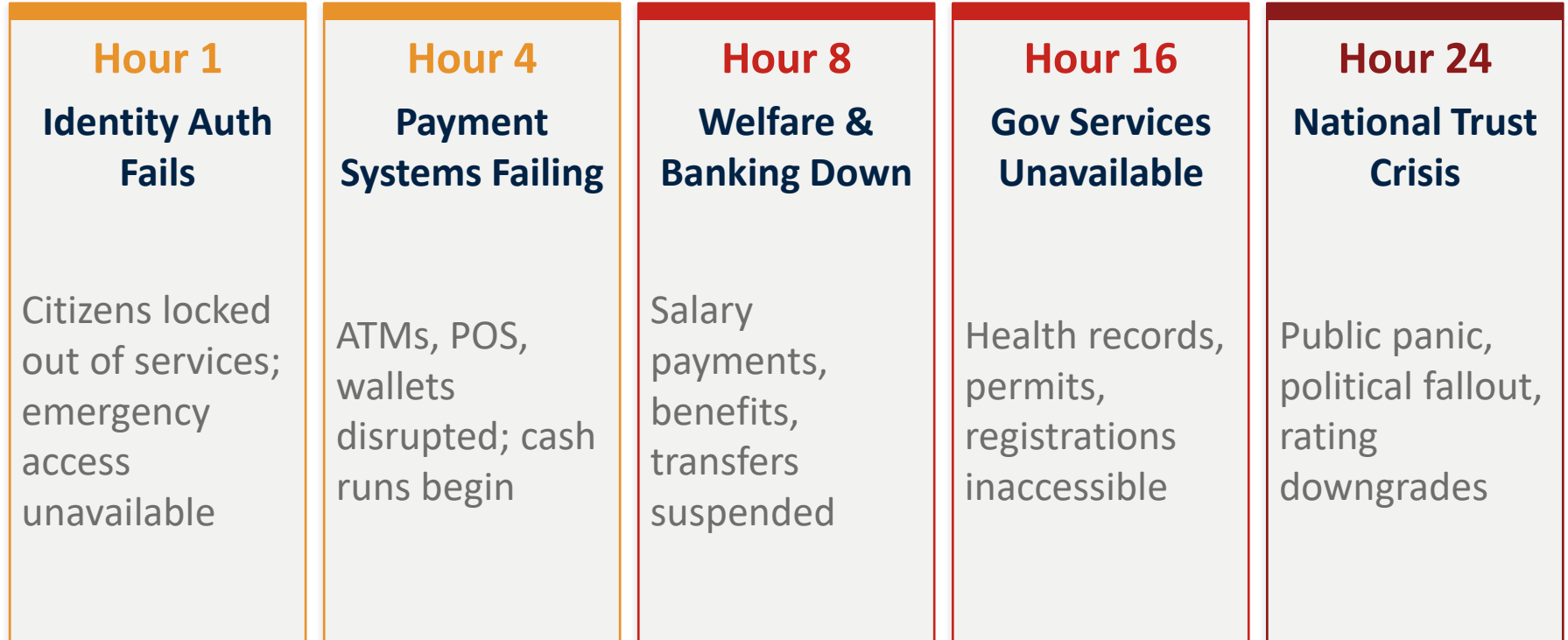
DPI operator controls access and identity layers

ARCHITECTURE

Foreign cloud and vendor infrastructure controls all

Architecture becomes power.

DPI Failure Simulation: First 24 Hours



From Risk to Reform

Six policy prescriptions for resilient, rights-respecting Digital Public Infrastructure

Mandatory Federated Architecture 01

No single operator controls the full DPI stack. Identity, payment and data exchange must be distributed with regulated interoperability.

Guaranteed Offline Fallback 02

Every DPI-gated public service must have a biometric-free alternative. No citizen may be excluded by authentication failure.

Judicial Oversight for Shutdown Powers 03

Internet shutdowns, payment suspensions and identity freezes must require a court order. Emergency powers must auto-expire.

Prohibition on Predictive Policing & LFR 04

Live facial recognition in public spaces and predictive surveillance scoring must require legislative mandate, judicial warrant and independent audit.

05

Data Sovereignty & Cloud Residency Rules 05

All citizen DPI data must be stored in sovereign jurisdiction. Cloud contracts must prohibit CLOUD Act-style foreign access. Portability mandatory.

Depoliticise DPI Governance

Insulate Identity Agencies from Electoral Cycles & State Capture

06

Transparent Governance

- ▶ Restore competitive, merit-based appointment process for DPI leadership (no political or military appointments)
- ▶ Multi-stakeholder DPI Council to advocate across political cycles
 - ▶ International partnerships can lock in reform continuity beyond single administrations

Citizen Data Rights

- ▶ Scale consent-based data sharing tools so citizens control who accesses their identity data
 - ▶ Mandate regular algorithmic & process bias audits for gender, disability, and social status discrimination

Anti-Capture Safeguards

- ▶ Anticipate elite pushback when DPI disrupts rent-seeking, tax compliance, voter rolls, proxy prisoner detection
 - ▶ Build coalitions from the outset with media and judiciary to expose opacity and sustain reform

Source: Tariq Malik, 'Digital ID for Development and Smart Governance: Policy Lessons, CGDev Note, 2025

DPI SAFEGUARD ARCHITECTURE

Tensions , Safeguard Pillars , Framework Anchors

Synthesised from UNDP-DP · WB-ID4D · UNDESA · UNTE-AI · CGAP · GovStack · ITU-CG · MOSIP

CROSS-CUTTING TENSIONS

Inclusion vs. Integrity

Centralisation vs. Resilience

Automation vs. Accountability

Access vs. Equity



FRAMEWORK ANCHORS

UNDP-DP

Digital Pathways Safeguards

WB-ID4D

ID Principles for Development

UNTE-AI

UN Tech Envoy AI Governance

UNDESA

e-Government & Open Data

CGAP

Digital Finance Consumer Prot.

GovStack

Building Block Specs

● Run Algorithmic Impact Assessments before every AI deployment

● Mandate open standards: FHIR / OpenID / X-Road across DPI stacks

● Establish data protection authority with enforcement powers

● Build USSD/IVR offline fallbacks as first-class requirements

Final Insight

DPI success increases state capacity

- + Well-designed DPI accelerates development, reduces inequality, and expands government reach to the unreached.

DPI dependency increases systemic risk

- ! As systems scale, efficiency gains can create new concentrations of control, dependency, and risk

Resilience must be designed deliberately

- > Resilience is not free. It requires investment, governance, and political will; before a crisis, not after.

DPI doesn't digitalize the State, it redistributes power within it



- Without safeguards, pro-poor governance concentrates, instead of serving citizens.

CORE INSIGHT

*The better DPI works,
the more catastrophic
its failure becomes.*

*The lesson is not to avoid DPI, but to avoid
fragile architecture and weak governance*

DPI Under Siege | ID4Africa Conference 2026 | ©Tariq Malik

APPENDIX

Sources & Reference

All figures presented as ranges where sources differ · Publicly available government, intergovernmental & peer-reviewed sources

A Global Frameworks & DPI Governance

- World Bank ID4D Principles (2017)
- OECD Digital Economy Outlook (2023–24)
- BIS Fast Payments & Financial Inclusion (2023)
- UN OHCHR Right to Privacy / Surveillance

B China — Social Credit & Surveillance

- PRC State Council Social Credit Plan (2014–2020)
- Creemers: Social Credit System (SSRN)
- MERICS Analysis Hub
- CSET Georgetown: Sharp Eyes Program

C India — Aadhaar Scale, Exclusion & Data

- UIDAI Official Statistics
- Drèze et al. — Welfare Exclusion (EPW)
- The Tribune: Data Breach Investigation (2018)
- Supreme Court Puttaswamy Judgment (2018)

D Africa — Shutdowns, Kenya & Ethiopia

- Access Now #KeepItOn Reports (2020–25)
- Internet Society Pulse: Ethiopia Tracker
- UN OHCHR Commission on Ethiopia (2022)
- GSMA State of Mobile Money (2023–24)

E EU / UK — LFR, Chat Control & eIDAS

- UK ICO LFR Guidance / Guardian: 90% false +ve
- EC Chat Control CSAR Proposal (2022)
- EU Council CSAM Position (2025)
- eIDAS 2.0 EUDI Wallet · EFF Art. 45 concerns

F Canada — Emergency Financial Measures

- Emergencies Act — Public Order Emergency
- ~210 accounts frozen; C\$7.8M (Forbes, 2022)
- Justice Canada Q&A on Emergencies Act
- Public Safety Canada Official Reports

G Pakistan — NADRA & DPI Outcomes

- NADRA Official Releases & Statistics
- State Bank of Pakistan — RDA Data
- BISP Programme Data
- CGD Note: Malik T. (2025) Digital ID Lessons

H Cloud Concentration & Sovereignty

- Synergy Research Group: Cloud Share (2024)
- Gartner Cloud Infrastructure Market (2023)
- OECD Cloud Computing Market Study
- U.S. CLOUD Act (2018)

I Cross-Cutting — Systemic Risk & Cyber

- ENISA Threat Landscape / Systemic Cyber Risk
- NIST Cybersecurity Framework
- Carnegie Endowment: Cloud Concentration Risks
- OHCHR Spyware & Surveillance Report (2022)

This appendix compiles publicly available sources from government publications, international organizations, peer-reviewed research, and verified investigative reporting.