Asia Pacific Policy Observatory 2026

Futures of Asia Pacific's Digital Public Infrastructure: A Youth-Led Study Co-created by Community

Governed for Whom? Accountability in the Asia Pacific Digital Public Infrastructure

Research Report

Organised by

NETMISSION.asia
www.nma.asia

Funded by

TWNIC

Supported by

yigf.asia
.asia Connecting Asia with One Domain
RECENT
TEEN IGF

Disclaimer

Youth researchers contributing to this report were permitted to use generative AI tools to support their work, including for language support, research assistance, and other purposes they deemed necessary. However, all final content reflects the researchers' original ideas and analysis. Direct copy-pasting of AI-generated content without meaningful review, interpretation, or authorship was not permitted. All contributions underwent human review and editing to ensure quality, accuracy, and alignment with the values of the initiative.

Whilst every effort has been made to ensure that the information contained in this report is accurate, neither the Asia Pacific Policy Observatory, NetMission.Asia, DotAsia Organisation nor TWNIC accept responsibility for any errors or omissions. Responsibility for the opinions expressed in the articles rests solely with the authors, who are also responsible for the contents of their articles, the accuracy of all quotations and their correct attribution, the accuracy of all citations and bibliographic listings, and the legal right to publish. The opinions expressed in the articles are those of the authors, and do not necessarily represent the views of the Asia Pacific Policy Observatory, NetMission.Asia, DotAsia Organisation, and TWNIC.

Research Coordinator
Sherry Shek

Project Coordinator
Bea Guevarra

Editor
Sherry Shek

Authors
Fatima Rezaie
Haris Ahmad Khan
Jeremy Htet
Khushbakht
Manas Joshi
Shiang Yen Eow

Contributors

The following contributed to this research through their questionnaire responses and/or participation in group discussions in the weekly research meetings. This list includes only those who consented to be named:

Abubakar Kamal
Aliza Mahar
Charlotte Hendro
Deeksha Agarwal
Easten Tato
Fatima Rezaie
Garv Chauhan
Gelie Esteban
Haris Ahmad Khan
Himaja Chanda
Jeremy Htet
Khushbakht
Manas Joshi
Maryam Khalid
Maulidya Alhidayah
Namratha M
Om Prakash Sharma
Omor Faruque
Prashansa Joshi
Rasleen Kaur
Rekha Angdembe
Sanjina Kshetri
Sohee Park
Yashika Sharma
Zakia Rahimi

Acknowledgements

We thank the following for sharing their expertise with the research group:

- Dmitry Kuznetsov, Postdoctoral Researcher, critical infrastructure lab (University of Amsterdam)
- Gyan Prakash Tripathi, Lawyer and Technology Policy Advisor

Table of contents

Key findings

The six studies compared how Digital Public Infrastructure (DPI) is governed across selected Asia Pacific countries, with a focus on accountability. Their central findings:

- Most governments state goals for their DPI but few track them (Haris Ahmad Khan). Quantified, time-bound targets are common, yet in Malaysia, Philippines, Nepal, and Pakistan they sit alongside missed deadlines and no independent monitoring, showing that a numeric target can signal intent but cannot on its own guarantee accountability.

- Few countries define DPI as a legal category (Shiang Yen Eow). Most regulate its components (digital identity, payments, data protection) without recognising DPI itself in law, and recognition consistently lags behind deployment. Among the examined countries, India's G20 Task Force framework is the clearest official definition, though not a statute.

- A **strong legal** and **regulatory foundation does not guarantee strong accountability** (Manas Joshi). In many countries, accountability is weak because there is no functioning consolidated oversight body. Only four countries, South Korea, Singapore, the Philippines and Australia, have both a data protection law and an authority that is already operational. India brought its law into force and constituted its Data Protection Board in November 2025, with member appointments currently underway. Pakistan is the exception, where it has the most detailed DPI law among the compared countries, but the authority created under the law cannot be judicially reviewed.

- **Formal public consultation**[1] is institutionalised in only a few countries: India, Australia, Nepal, and Papua New Guinea (Jeremy Htet). Most others rely on ad-hoc, **expert-driven, sectoral consultation** or project-tied engagement rather than a standing channel through which citizens can shape the systems. Moreover, DPI designing and implementation process is largely driven by **international collaboration and bi-lateral partnerships**, with most countries relying on global financial institutions and partnerships such as the World Bank and Asia Development Bank, rather than acting alone. This highlights the central role of **cross-border collaboration** in building scalable digital systems, especially in developing countries.

[1]In this study, formal consultation mechanism is defined as a structured, official process through which governments systematically collect, document, and utilize multi-stakeholder feedback to guide Digital Public Infrastructure (DPI) design, implementation, and regulation.

- Having a law does not mean citizens are protected, and publishing information does not mean a system is accountable (Khushbakht). What matters is whether people can seek remedy when a system fails them and find out how it works. On remedy, Australia is the only country with a dedicated statutory redress mechanism; Pakistan built its DPI at scale while closing that route by statute, so that when a data breach exposed the records of 2.7 million citizens, they had no channel to seek redress. On transparency, South Korea discloses more about its DPI than any country in the set, but much of that is routine administrative paperwork rather than substantive policy, and citizens were still left without recourse during a major 2023 outage.

- Where nothing constrains them, identity and data systems built for service delivery become instruments of monitoring and control, most severely in Afghanistan and Myanmar (Fatima Rezaie). She argues that the capacity of civil society to scrutinise these systems is the factor most consistently associated with better outcomes across the ten countries she examines.

About the APPO 2026 Project

APPO 2026 is the latest edition of the Asia Pacific Policy Observatory (APPO), a youth-led research initiative on the governance of the internet and emerging technologies, run by NetMission. It has two aims meant to advance together: to build the capacity of youth policy researchers, and to produce research on digital policy that reflects their perspectives and priorities.

Members join with varied expertise: some are students, others are working professionals in policy, law, and technology. Capacity building here is built into the research rather than run alongside it as a separate set of workshops. Members develop and apply the skills the work requires (research design, data analysis, and evidence-based writing) through weekly meetings from March 2026 to May 2026 with the Research Coordinator, joined periodically by guest expert speakers, as they carry out the research.

Understanding of Digital Public Infrastructure (DPI) is built the same way, through the research rather than before it. Each author defines their own dimension, sets the standard against which countries are compared, and carries out the analysis, drawing on their lived experience and knowledge of their own contexts; the Research Coordinator provides the overall design and draws the studies together. The group's grasp of DPI governance and accountability grows as the studies take shape.

About the research

This report presents the findings of APPO 2026 on how DPI is governed across selected APAC countries, with a focus on accountability. It comprises six studies, each written by a member of the research group and covering one or two governance dimensions.

The research began with two broad questions. The first was about power and accountability: how decisions about DPI are made, what mechanisms exist for public input and oversight, and how power over these systems is checked. The second was about values: whether concerns such as privacy, security, inclusion, and efficiency figure in how DPI is governed, and whether accountability mechanisms reflect them or are missing altogether. These were the starting points.

The specific questions the studies answer, together with the Asia Pacific countries to cover, emerged from the questionnaire responses collected during the recruitment of voluntary research group members (aged 18-35) in February 2026. The sign-up form for this research project doubled as a questionnaire: each prospective member indicated a country they were interested in and answered questions about DPI governance, such as whether consultation exists, drawing on their own knowledge and brief research.

In total, 36 responses covering 14 countries were collected. The countries included are: Afghanistan, Australia, Bangladesh, China, India, Indonesia, Malaysia, Myanmar, Nepal, Pakistan, Papua New Guinea, Philippines, Singapore, and South Korea.

The design served two purposes. It crowdsourced DPI information from the youth community, drawing out the accountability issues members saw in their own contexts; and it grounded the research in countries that group members already know and have an interest in. The Research Coordinator then consolidated the responses and identified the concerns that recurred across them.

The research is organised around governance dimensions. A dimension is one aspect of how DPI is governed, examined the same way across all selected countries so they can be compared on it. The dimensions the studies examine emerged from the Research Coordinator's consolidation of questionnaire responses rather than from a predetermined framework, sharpening the two starting questions into a set the studies could answer:

- whether governments state and track what their systems are for,
- whether those systems are grounded in law and overseen by independent bodies,
- whether people can shape them, see how they work, and seek remedy when they fail, and,
- what happens to citizens when these checks are absent.

This report completes the first phase of the project: a broad comparison designed to surface patterns across the selected countries. The next phase builds on these findings, narrowing to comparative case studies, comparing specific DPI systems between country pairs that are identified as analytically significant.

About the authors

Fatima Rezaie
Fatima Rezaie is an Afghan education activist and public policy professional dedicated to expanding educational opportunities for women and girls. She earned a Bachelor's degree in Political Science and Public Administration from the American University of Beirut and a Master of Public Affairs (MPA) from Brown University. She is the founder of Educate2Empower, an online platform that connects women in Afghanistan with scholarships, educational resources, mentorship, and academic opportunities, helping them pursue higher education despite significant barriers. Through her advocacy, mentorship, and digital outreach, she works to empower Afghan youth and promote equitable access to education.

Haris Ahmad Khan
Haris is a UCL grad and a futurist. He has experience and is curious about emerging technology, experiences, design, moonshot & related areas to create synergies using transdisciplinary praxis towards redefining planetary civics, prosperity & regenerative futures.

Jeremy Htet
Jeremy is a graduate student in Development Studies at Chiang Mai University with a background in anthropology and a strong interest in the intersection of technology and social issues, including digital public infrastructure, internet governance, and AI. He has experiences in research coordination, and youth leadership across APAC region and beyond.

Khushbakht
Khushbakht is an electrical engineer from Pakistan researching digital public infrastructure and AI governance. She is particularly interested in how accountability is designed into public digital systems, and how that shapes people's ability to understand, challenge, and trust them.

Manas Joshi
Manas is a technology and public policy professional working on AI governance, inclusive digital public infrastructure, Universal Acceptance and multilingual internet access. He has experience across the private, social and public sectors, and is currently working on frontier-technology and digital governance policy in India. .

Shiang Yen Eow
Shiang Yen is a postgraduate student in Community Nutrition at Universiti Putra Malaysia, an Executive Committee member of the Malaysian Youth Council, and researcher at INITIATE.MY. His work focuses on the SDGs, social cohesion, freedom of religion or belief, digital rights, peacebuilding, and interfaith engagement through research and advocacy.

Research approach

Country coverage varies between the six studies. Most span all **14 countries**, though some cover fewer. The method, data collection, and limitations set out in the following are common to the six studies; where a study departs from them, or has details specific to the study, they are noted in that study.

Method

The process was iterative rather than linear. It did not move in sequence from a theory to a framework to data collection to analysis; it moved back and forth between the group's own knowledge of DPI, the questions to ask, and the data collected, with each round reshaping the next. It was grounded in the perspectives of the youth community, starting from what members already knew about DPI in the countries they chose.

That knowledge was gathered through the recruitment questionnaire, which doubled as the first round of data collection. Members answered questions about the DPI governance of a country they chose:

- how the government defines DPI,
- when DPI first entered policy discussion,
- what DPI systems exist,
- whether public consultation is part of DPI policy-making and how it is carried out,
- what regional DPI partnerships the country takes part in, and
- what was hardest to find information about.

The Research Coordinator consolidated these responses anonymously for the group to read, and members were asked to note patterns, outliers, and possible explanations. The responses fed into the group's weekly meetings, where a continuous discussion gradually shaped both the research questions and what data to gather next.

The discussions also crystallised what each dimension should capture, which each study then sets out at its start. Each study follows the same qualitative comparative method. It defines its governance dimension, sets a baseline against which countries can be compared, assesses each country against that baseline, and groups the countries into clusters that make the patterns visible.

Data collection

The primary data are the governance instruments themselves: the government's published regulatory documents and legislation, through which DPI is defined and governed. International-organisation reports, civil-society and digital-rights reports, academic literature, and journalism serve as secondary material, used to validate the primary documents and to supplement them where these are inaccessible.

Members recorded these sources in a shared collaborative spreadsheet, one row per document capturing its type, author, publication details, a link for citation import, and the countries it concerns, with a linked sheet holding the quotes and passages drawn from each.

As sources were gathered, members annotated them against the research questions, tagging each annotation to the governance dimension it spoke to and to the claim it supported, contradicted, or complicated. This let the group see, dimension by dimension, where the data were thin or where sources conflicted. Most sources date from 2019 to early 2026, the majority from 2022 to 2026, with a few earlier works retained where they establish a definition or a baseline. The data are predominantly in English.

Limitations

Several limitations apply across the studies. With the dominance of English-language data, domestic-language debate and civil-society critique in other languages are under-represented. Coverage is also uneven in quality: it is strongest for countries with accessible public documentation, such as India and Singapore, and weakest where government documents are scarce or cannot be taken at face value, such as Afghanistan and Myanmar; in those cases the studies rely more heavily on secondary material. Finally, the findings are a snapshot of early 2026, as several countries revised their legal frameworks during the research period; the studies note these changes where relevant.

Reflexivity note

The researchers joined the research group with local knowledge and experience, as well as concerns about governance accountability in their home countries. This equipped the analysis with practical insights on the one hand, and on the other, may have introduced interpretive bias. This was treated with caution, notably through regular meetings where the researchers shared findings and interpretations that were then challenged and discussed.

Introduction

International organisations describe digital public infrastructure (DPI) as the foundational, society-scale digital systems underpinning public and economic life. The World Bank, the United Nations Development Programme (UNDP), and the Digital Public Goods Alliance (DPGA) each characterize DPI systems as building blocks that support public services and economic participation (DPGA, 2024; UNDP, 2023; World Bank, 2025). India's G20 Task Force gives one of the most cited official statements, framing DPI as an ecosystem of identity, payments, and data exchange together with the institutional and legal arrangements around them (India G20 Task Force on Digital Public Infrastructure, 2024).

These definitions treat DPI as more than technology. It is a socio-technical system whose positive impacts depend on governance: the legal safeguards and institutions around the technical layers. Consequently, it should aspire towards open standards and interoperability, protect privacy by design, reach people inclusively, and be governed transparently and accountably to the population it serves rather than only to the state that runs it (UNDP, 2023; World Bank, 2025).

Mazzucato et al. (2024) argue that DPI is genuinely public only if it embeds public value, and Eaves and Rao (2025) treat embedded public-interest values, alongside the underlying technology and societal adoption, as a dimension on which DPI should be judged.

This report asks a different question: whether the people who depend on these systems can trust them. Trust, here, means being able to find out how a system works, to help shape it, and to get help when it fails. That is a question of accountability, and it runs through the six studies included in this report.

Why accountability matters

DPI concentrates a population's identity and payment records into systems the state can see and act on. When accountability is absent, the same infrastructure that delivers a service can be turned on the people it serves: Fatima Rezaie's study of surveillance traces how identity and data systems built for service delivery become instruments of monitoring and control once nothing constrains them. Even without any intent to misuse, the cost of failure lands unevenly. As Khushbakht shows, when a biometric read fails or a payment is wrongly blocked, it is the household with the least recourse, cut off from welfare with nowhere to complain, that pays. Accountability matters first because its absence is felt hardest by those least able to absorb it.

Beyond the immediate harm, accountability is what makes DPI legitimate and durable. It is the line between infrastructure that is genuinely public and infrastructure that is public only in name: a distinction Khushbakht draws on, between a citizen and a mere user. It is also what lets a system be judged at all. Haris Ahmad Khan shows that without stated goals there is no standard to hold a government to, and no basis on which to audit or compare. And at population scale,

Manas Joshi argues, the weaker the legal foundation and oversight, the more infrastructure is deployed without a commensurate check, and trust erodes with it.

What accountability is made of

The studies engage with accountability through two intertwined components: answerability, the duty to explain and justify how a system is run; and enforcement, the capacity to impose consequences and provide remedy when it fails. A grievance channel with no power to compel a remedy is answerability without enforcement. An oversight body that never has to explain itself is enforcement without answerability. Both are needed to ensure accountability.

The structure of accountability

Read this way, the six studies trace the structure of accountability, exploring its preconditions, its mechanisms, and its absence.

Two studies are about preconditions of accountability. Haris Ahmad Khan examines the goals a government states for its DPI, the standard any system must be judged against, and finds targets that are rarely tracked. Shiang Yen Eow examines whether DPI is recognised as a legal category at all, and finds explicit definitions rare. Three studies look into the mechanisms accountability works through: Manas Joshi maps the legal foundations and oversight bodies that can enforce; Jeremy Htet examines consultation, the channel through which people shape a system, and finds it confined to a few countries while the rest rely on ad-hoc engagement; and, Khushbakht takes grievance redress and transparency, the mechanisms that let people seek remedy and see how a system works. The last study argues what their absence produces: Fatima Rezaie's study of surveillance, where power over citizens runs without a check.

Form and function

A recurring pattern across these studies highlights that accountability on paper does not guarantee accountability in practice. A country can define DPI, publish goals, pass a statute, and name an oversight body, and still leave citizens unable to shape the system, seek remedy, or see how it works. It appears most sharply in Manas Joshi’s account of legal foundations, in Haris Ahmad Khan’s finding that a quantified target is a governance signal rather than a governance mechanism, and in Khushbakht’s Pakistan case. As a broad first-phase comparison, these studies map that gap rather than resolve it.

1. Stating Without Steering: National DPI Goals and the Accountability Gap Across Asia-Pacific States

By Haris Ahmad Khan

Background and literature

The question of what a government says its digital public infrastructure is for has received less comparative attention than questions about what DPI does or how well it works. Most governance research focuses on implementation maturity, legal frameworks, or accountability mechanisms. Goal articulation, the publicly stated purposes a country assigns to its DPI systems, is typically treated as background rather than subject. This study argues that stated goals deserve direct analytical attention. How a government frames its DPI intent is itself a governance indicator.

The most analytically precise framework for evaluating DPI goals comes from Mazzucato, Eaves, and Vasconcellos (2024), who argue that DPI must embed public values to constitute genuinely public infrastructure. Among the five pillars they propose, two are directly relevant to goal articulation. The first is purpose and directionality, which asks what the system is pointed at and who decided. The second is transparency and accountability, which asks whether goals are documented in ways that allow citizens to evaluate whether they have been met. Their argument implies that DPI without stated goals, or with goals stated only in technical rather than civic terms, cannot be held to a public standard.

Eaves and Rao (2025) offer a measurement framework that makes this concrete. They define DPI across three dimensions: underlying technology, embedded public-interest values, and societal adoption context. Goal articulation falls within the public-interest values dimension. A system that scores highly on technological deployment but poorly on public-interest values, including whether goals are publicly stated and monitored, represents what they describe as incomplete DPI.

Seth, Vitagliano, Udupa, and colleagues (2023) take a more critical position, drawing on India's experience. They find that the absence of formally stated goals, or the statement of goals without accompanying oversight mechanisms, concentrates risk in the communities least able to absorb it. Marginalised populations excluded from welfare benefits by biometric failures have no recourse when the system's stated purpose is not legally enforceable. The governance framework they propose requires public oversight across three phases: conceptualisation, technical design, and active management.

A separate thread in the literature concerns how DPI goals are framed, not simply whether they exist. The India G20 Task Force report (India G20 Task Force on Digital Public Infrastructure,

2024) frames DPI goals as encompassing digital identity, payments, data exchange, institutional arrangements, legal safeguards, and market participation. This is a civic enabler framing. By contrast, the CAICT report on China's DPI practices frames goals around national security, infrastructure modernisation, and data centralisation under party-state direction (CAICT, 2025). The framing is not incidental. It determines what accountability architecture is built, who can challenge DPI decisions, and what counts as success.

A competing perspective holds that DPI goals in developing states are best evaluated as development instruments rather than civic commitments. The GDN working paper on Bangladesh (Raihan et al., 2025) assesses DPI through a socioeconomic development lens, measuring impact on economic activity and inclusion rather than governance quality. This framing is coherent within its own terms, but it makes goal accountability harder to assess.

The existing literature is weakest on goal articulation as a comparative dimension across APAC specifically. Research on India and Singapore is substantial. Research on goal-setting in smaller or more politically constrained states, including Myanmar, Nepal, Bangladesh, Afghanistan, and Papua New Guinea, is thin or scattered across grey literature. This interim comparison addresses that gap directly, across all fourteen countries in the dataset.

Table 1: Three Paradigms of DPI Goal Framing in the Literature Summarised

	Civic Enabler	Development Outcome	State Control
How goals are framed	Public good; rights-based; access to services as civic entitlement	Instrument for poverty reduction, financial inclusion, and economic growth	Tool for administrative control, national security, and data centralisation
Key literature	UNDP (2023); World Bank (2025); Mazzucato et al. (2024); Seth et al. (2023); Eaves & Rao (2025)	Raihan et al. (2025); NASSCOM (2024); World Bank DEEP (2025)	CAICT (2025); MoTC Myanmar (2024)
Countries in this study	India, Singapore, South Korea, Australia, PNG	Indonesia, Bangladesh, Nepal, Pakistan	China, Myanmar, Afghanistan
Accountability implied	Goals should be enforceable; citizens can challenge DPI decisions	Goals measured by development outcomes; harder for citizens to challenge	Goals are state prerogative; no public accountability expected or provided

Definition and baseline for this study

In plain terms, a stated national DPI goal is a publicly documented commitment by a government describing what its foundational digital systems are meant to achieve, for whom, and by when. This definition focuses on articulation, not implementation. A country may have advanced DPI systems without clearly stated goals, or clearly stated goals with minimal implementation. This comparison focuses on what governments say, not only what they build.

This dimension matters for DPI governance because accountability begins with articulated intent. A DPI system without stated goals cannot be evaluated against any standard. It cannot be challenged by citizens, audited by independent bodies, or compared across borders. Seth et al. (2023) put this plainly that without publicly stated goals and oversight, DPI systems operate on the terms of those who build them, not those who depend on them.

The definition draws on the G20 Task Force framework (India G20 Task Force on Digital Public Infrastructure, 2024), which treats DPI goals as covering at minimum three layers: what the identity infrastructure is for, what the payment infrastructure is for, and what the data exchange infrastructure is for. A complete statement of national DPI goals addresses all three, ties them to measurable outcomes, and specifies a body responsible for tracking progress.

Three-tier baseline

Tier 1 describes countries whose goals exist and are subject to some accountability or monitoring mechanism. That mechanism may be statutory review, an independent body, or administrative procedure. The form of the document is not the test. Australia qualifies through statutory regulatory impact assessment. South Korea qualifies through the Administrative Procedures Act, despite having no dedicated DPI strategy document.

Tier 2 describes countries whose goals exist, sometimes with specific numeric targets, but where no functioning accountability or monitoring mechanism tracks whether those goals are met.

Tier 3 describes countries where no accessible DPI goal documentation exists in civilian-oriented form, where pre-existing goals have been made defunct by political change, or where stated goals are oriented primarily around state control and surveillance rather than public service delivery.

This baseline was chosen because it allows comparison across countries at very different stages of DPI development without requiring all countries to meet the same threshold. It also separates two things that are easy to conflate: the existence of numeric targets and the existence of accountability infrastructure.

It is important to note that Tier 3 does not imply the total absence of stated goals. In Myanmar's case, the military government has published formal DPI strategy documents. The Tier 3

classification reflects that these goals serve state control rather than citizen benefit, and that no civilian-oriented or publicly consultative DPI strategy exists alongside them.

Table 2: Three-Tier Baseline for Comparing Stated National DPI Goals

Tier	Defining Criteria	Countries	Key Characteristic
Tier 1	Goals exist and are subject to an accountability or monitoring mechanism (statutory review, independent body, or administrative procedure). Document type is descriptive, not the test.	India, Singapore, South Korea, Australia, PNG	Goals institutionalised through legal or governance architecture
Tier 2	Goals exist, sometimes with numeric targets, but no functioning accountability or monitoring mechanism tracks them.	Malaysia, Philippines, Nepal, Pakistan, Indonesia, Bangladesh	Quantified goals without accountability infrastructure — the quantification paradox
Tier 3	Goals absent, inaccessible, or oriented primarily toward state control rather than citizen benefit	China, Myanmar, Afghanistan	Goals serve the state, not the citizen; civilian-oriented DPI strategy is absent

Data collection

Sources span a date range from 2009 through early 2026, with the majority from 2022 to 2026. The evidence base is predominantly in English. This is a significant gap. Domestic policy debates in Korean, Mandarin, Burmese, Bahasa Indonesia, Nepali, Urdu, Bengali, Dari, and Pashto are not captured. Country coverage is uneven. India, Singapore, Australia, and Pakistan have rich documentation. Myanmar and Afghanistan are structurally difficult to research. The source base for Pakistan and PNG reflects rapidly changing conditions: the Digital Nation Pakistan Act was enacted in January 2025 and SevisPass launched in November 2025.

Table 3: Source Coverage by Country Relevant to Stated National DPI Goals

Country	Sources	Govt Primary Docs	Independent Analysis	Overall Coverage
Pakistan	9	Yes	Yes (World Bank, DRF, ICLG)	High
India	7	Yes	Yes (NASSCOM, Seth et al., CSEP)	High
Myanmar	8*	Partial	Yes (IFEX, IMS, Chatham House)	Low
Afghanistan	7	None	Yes (IMS, SEAP, UNEP)	Low
Indonesia	6	Yes	Yes (Sarjito & Thamrin, Bachtiar)	Moderate
Singapore	5	Yes	Yes (World Bank + GovTech)	High
South Korea	5	Yes	Yes (OECD)	High
Malaysia	5	Yes	Partial (OpenGlobalRights, PwC)	Moderate
Australia	4	Yes	Yes (OECD, APRA)	High
China	4	Partial	Limited (CAICT is semi-government)	Moderate
Philippines	3	Partial	Moderate (DPGA, OGP)	Moderate
Nepal	3	Partial	Limited (Biometric Update, Lexology)	Low-Moderate
Bangladesh	2	Partial	Moderate (GDN, DCO)	Low-Moderate
PNG	2	Yes	Limited (SevisPNG documentation only)	Moderate

** Myanmar's high source count is inflated by surveillance and infrastructure-control documents (CEIR, Cybersecurity Policy, PSMS). The coverage quality for civilian-oriented DPI goals is low.*

Findings

The fourteen countries fall into four patterns based on how their national DPI goals are articulated, framed, and monitored. The comparative table below provides a summary overview, followed by analysis by cluster.

Table 4: Comparative Overview of Stated National DPI Goals

Country	Stated Goals Summary	Tier
India	India Stack (Aadhaar, UPI, DigiLocker); public services, government efficiency, digital economy. UIDAI established 2009. Goals stated programmatically, not through a single statute.	Tier 1
Singapore	Smart Nation: service delivery, financial inclusion, digital economy via Singpass and PayNow. Goals institutionalised through operational systems rather than declaratory documents.	Tier 1
South Korea	Government efficiency and administrative modernisation via 5-year plans. Framework Act on Intelligent Informatization. No dedicated DPI strategy document.	Tier 1
Australia	Data and Digital Government Strategy 2023-2030; Digital ID Act 2024; phased public review; statutory regulatory impact assessments required.	Tier 1
Papua New Guinea	Digital Government Plan 2023-2027; National Digital ID Policy 2025; SevisPass and SevisWallet launched November 2025. Goal: first decentralised DPI ecosystem in Oceania.	Tier 1 (emerging)
Malaysia	95% of government services online by 2030 (MyDIGITAL). MyDigital ID, DuitNow, PADU. No independent monitoring body; intermediate milestones not tracked publicly.	Tier 2
Philippines	125,000 WiFi sites by 2028; PhilSys digital ID; E-Governance Act (RA 12254, 2025). Goals expressed through sector-specific legislation, not a unified DPI strategy.	Tier 2
Nepal	99% internet penetration target; National ID, National Payment Switch, Nagarik App. Digital Nepal Framework. Deadlines routinely missed; no monitoring body.	Tier 2
Pakistan	DPI first by 2035; Pakistan Stack (identity, payments, data exchange) under Digital Nation Pakistan Act 2025. Primarily framed as development and financial inclusion outcome.	Tier 2
Indonesia	Service delivery, financial inclusion, digital economy via SPBE framework (Presidential Regulation No. 82/2023). QRIS as most concrete DPI-specific goal. Goals nested in e-gov policy.	Tier 2

Bangladesh	Smart Bangladesh 2041; NID system, EkPay, government data exchange. DPI framed as development and economic growth tool. Project-by-project rather than consolidated strategy.	Tier 2
China	National security, data centralisation, administrative control. DPI as 'New Infrastructure' (Xin Jichu) under NDRC. Clearly stated and sustained; no public consultative framing.	Tier 3
Myanmar	e-Governance Master Plan 2030 (MoTC, 2024) states goals around modernising public administration. No civilian-oriented strategy. In practice infrastructure directed toward surveillance and population control.	Tier 3
Afghanistan	No accessible stated goals since 2021 Taliban takeover. Pre-2021 e-governance frameworks defunct. Digital infrastructure used for censorship and surveillance.	Tier 3

Cluster A: Institutionalised Goals

Cluster A maps to the Tier 1 definition. India, Singapore, Australia, South Korea, and Papua New Guinea have the clearest formally stated and institutionally anchored DPI goals subject to an accountability or monitoring mechanism. They arrive at this position through different legal and governance pathways.

India's goals are articulated through the India Stack architecture and the UIDAI mandate established in 2009, rather than a single DPI statute. The India G20 Task Force report (India G20 Task Force on Digital Public Infrastructure, 2024) provides the most comprehensive official articulation: DPI as an ecosystem of identity, payments, data exchange, institutional arrangements, legal safeguards, and market participation. The framing is explicitly civic.

However, Seth et al. (2023) document that goals stated at this level of abstraction, without enforcement mechanisms, have produced exclusion of marginalised communities from welfare systems. Institutionalisation and outcome monitoring are not the same thing. India's goals are institutionally anchored, because they are embedded in durable and operational architecture. The monitoring of outcomes, including who is excluded, is weak.

Singapore's stated goals are embedded in the Smart Nation initiative and implemented through Singpass, PayNow, and integrated e-government services. The World Bank and GovTech case study (World Bank and GovTech Singapore, 2022) describes the system as one in which digital identity and payments are deeply integrated into public and private service delivery. Goals here are institutionalised through operational systems rather than declaratory strategy documents.

Australia has the most clearly documented goal architecture in this dataset, meaning the combination of documents, legislation and institutions through which a country states and pursues its DPI goals. The Data and Digital Government Strategy 2023 to 2030 sets phased implementation targets reviewed publicly. The Digital ID Act 2024 provides statutory grounding

for the identity layer, and the regulatory impact assessment process (Australian Prudential Regulation Authority, n.d.) requires structured cost-benefit analysis for all major digital regulations. Australia is the only country in this set where stated goals are linked to a statutory review and redress mechanism.

South Korea shows that Tier 1 does not require a dedicated DPI strategy document. Its digital governance goals are embedded in five-year administrative planning cycles, and the Framework Act on Intelligent Informatization provides the statutory basis (OECD, 2025). Goals are accountable through the Administrative Procedures Act. The OECD (2025) review notes that public consultations often occur too late in the policy process to meaningfully influence decisions, which is a real limit, but the accountability mechanism exists.

Papua New Guinea is the newest entrant. The Digital Government Plan 2023 to 2027 was mandated by the Digital Government Act 2022, which is primary legislation rather than a development framework. The National Digital Identity Policy 2025 launched SevisPass and SevisWallet in November 2025 with published assurance standards setting a tiered identity model (Department of Information and Communications Technology [PNG], 2025b). The statutory basis and published standards are the grounds for a Tier 1 placement. The monitoring claim is provisional because the system launched weeks before this analysis and has no track record yet. PNG is therefore marked Tier 1 (emerging).

Cluster B: Quantified but Under-monitored

Malaysia, the Philippines, Nepal, Pakistan, Indonesia, and Bangladesh have stated goals with varying degrees of specificity, but share a common accountability gap. Goals exist, and in some cases are quantified, but there is no independent monitoring mechanism to track whether they are being met.

Malaysia commits to 95% of federal services online by 2030 under the MyDIGITAL Blueprint (Ministry of Digital Malaysia, 2025). The goal is concrete and time-bound. But the 2b observations note that intermediate milestones are not tracked publicly and no independent monitoring body exists.

This points to a wider pattern. A stated goal of expanding digital access can run alongside a separate goal of expanding control, and reading only the headline goal misses that. Malaysia's Online Safety Act 2025 introduces new restrictions on online anonymity and content at the same time as its access targets expand (Amir, 2026). Goal framing has to be read critically, because the stated goal is rarely the whole intent.

Similar tensions appear in China, Pakistan, and India, so this is a regional pattern rather than a Malaysia-specific one.

Pakistan's Digital Nation Pakistan Act 2025 (Government of Pakistan, 2025) establishes a three-layer Pakistan Stack covering identity, payments, and data exchange, with a national

ambition described in the research observations as DPI first by 2035. This is one of the most formally stated DPI goal architectures in the dataset, enacted through primary legislation.

But the World Bank implementation status report (World Bank, 2025b) shows that as of December 2024, every implementation indicator for the parallel World Bank Digital Economy Enhancement Project reads zero. Pakistan has the most explicitly stated goals among Cluster B countries, and the largest documented gap between what is stated and what is being built.

Indonesia and Bangladesh sit at the lower end of this cluster. Indonesia's goals are embedded in the SPBE framework under Presidential Regulation No. 82 of 2023. Sarjito and Thamrin (2026) demonstrate that the SPBE framework is explicitly non-binding, which means goals lack legal enforceability. Bangladesh's Smart Bangladesh 2041 vision frames DPI as a development and economic growth tool, with the GDN working paper (Raihan et al., 2025) documenting the NID system, EkPay, and government data exchange as core layers.

Cluster C: State-controlled or Absent

China, Myanmar, and Afghanistan share the characteristic that their stated DPI goals, where they exist, are not oriented toward citizen benefit and are not subject to any form of public accountability.

China's goals are the most clearly stated of the three. The CAICT report (2025) frames DPI goals around national security, data centralisation, and administrative control under party-state direction. The New Infrastructure agenda, managed through the National Development and Reform Commission, sustains these goals across successive five-year plans.

Myanmar requires careful treatment. It is often described as having no stated DPI goals since the 2021 coup. That characterisation is inaccurate. The Myanmar e-Governance Master Plan 2030 was published in 2024 by the Ministry of Transport and Communications (MoTC, 2024) and contains stated goals around modernising public administration and digital government infrastructure. What is absent is civilian input, democratic framing, and any accountability mechanism.

The IFEX report (2025) documents the Person Scrutinization and Monitoring System, which combines facial recognition, AI, and digital IDs to surveil civilians, and the 2025 Cybersecurity Law, which criminalises VPN use and mandates unrestricted government data access from platforms. A separate India-Myanmar Memorandum of Understanding signed in July 2025 (Liang, 2025) commits India to supporting a Myanmar digital ID pilot, illustrating how stated goals of one government can be enrolled into the DPI export agenda of another regardless of how those goals are implemented domestically.

Afghanistan has no accessible stated DPI goals since the Taliban takeover in 2021. Pre-2021 e-governance frameworks exist on paper but are defunct. The IMS report (Flensburg, Lai, and

Lehmann-Jacobsen, 2025) documents how digital infrastructure is now used for censorship and surveillance.

The quantification paradox

Countries with specific numeric targets do not necessarily have stronger accountability than those without them. Malaysia, the Philippines, Nepal, and Pakistan all have quantified, time-bound goals. All four also have documented records of missing those deadlines with no consequences, and none has an independent body monitoring progress. India and Singapore have less quantified public targets but more deeply institutionalised DPI architectures that are operationally accountable.

A government announcing 95% digital service coverage by 2030 is not demonstrating accountability unless it also builds the monitoring infrastructure to track and enforce that commitment. The announcement is a governance signal, not a governance mechanism.

The most important takeaway

The framing of DPI goals is as informative as their content. Countries that frame goals around civic enablement tend to build different accountability structures than those that frame them around development outcomes or state control. Goal articulation is not merely descriptive. It is constitutive of what kind of DPI system a country builds.

Table 5: Positioning Matrix — Goal Specificity and Monitoring Infrastructure

	Monitoring Infrastructure: Weak or Absent	**Monitoring Infrastructure: Present or Strong**
Goal Specificity: Institutionalised (Tier 1)	South Korea, India, Singapore, PNG Goals embedded in governance cycles or operational systems without strong public monitoring mechanisms	Australia Formal strategy, statutory review, and public monitoring through regulatory impact assessments and the Digital ID redress framework
Goal Specificity: Quantified Targets (Tier 2)	Pakistan, Malaysia, Philippines, Nepal, Indonesia, Bangladesh Numeric targets stated; implementation behind schedule; no independent body monitoring progress	— No country in this dataset combines high numeric specificity with strong independent monitoring
Goals: State-directed or Absent (Tier 3)	China, Myanmar, Afghanistan Goals serve state or security interests; no civilian-oriented accountability structure exists	—

Limitation

Most sources are in English. Domestic debates in Korean, Mandarin, Burmese, Bahasa Indonesia, Nepali, Urdu, Bengali, Dari, and Pashto are not represented. For countries like China and South Korea, some official documents were translated rather than read in the original, which may introduce interpretive gaps.

Country coverage is uneven. Afghanistan and Myanmar are structurally difficult to research. For Afghanistan, the near-total absence of independent primary sources since 2021 means the analysis relies heavily on external reports. For Myanmar, the military government's own documents must be read against civil society reporting that documents how they are applied in practice.

This comparison cannot assess whether stated goals are achieved. It only assesses whether they are stated, how they are framed, and whether accountability mechanisms exist to monitor them. The gap between stated and implemented goals is a question for the next phase of the project.

2. How Is Digital Public Infrastructure Defined? Legal Recognition Across the Asia-Pacific

By Shiang Yen Eow

Background

DPI is increasingly understood as a socio-technical ecosystem rather than a purely technological infrastructure. Effective DPI requires not only technical systems but also governance arrangements, legal safeguards, institutional accountability, public trust, and market participation. Consequently, questions concerning statutory recognition and legal frameworks have become increasingly important in discussions surrounding DPI governance.

However, no universally accepted statutory definition of DPI exists. Countries have adopted different legal and governance approaches depending on their administrative traditions, institutional capacities, and digital development trajectories. Some countries have embedded DPI concepts within comprehensive legislative frameworks, while others rely primarily on executive policies, digital transformation strategies, or sector-specific regulations. Therefore, understanding how DPI is recognised and defined within national legal systems remains an important area of comparative policy research to allow communication, comparison, and understanding of context and nuances.

Definition and baseline for this study

For the purposes of this study, “Statutory DPI Definition” refers to the extent to which a country's legal, regulatory, or authoritative governmental framework explicitly recognises, defines, or conceptualises DPI or its equivalent foundational digital systems (Digital Public Goods Alliance, 2022).

This dimension focuses on legal and institutional recognition rather than technological sophistication. A country may possess highly advanced digital systems while still lacking formal legal recognition of DPI as a governance concept.

Four levels of statutory maturity

Level 1: Advanced Recognition and Formal Definition

Countries that provide explicit definitions of DPI or equivalent digital infrastructure concepts through legislation or authoritative government frameworks and establish clear governance principles.

Level 2: Composite Statutory Frameworks

Countries that do not explicitly define DPI as a single concept or have a single DPI law but maintain strong statutory foundations through an interconnected base of enacted primary legislations governing digital identity, digital payments, cybersecurity, interoperability, data governance, and digital public services.

Level 3: Executive and Policy-Led Recognition

Countries that lack a primary legislative base for digital infrastructure, relying instead almost entirely on executive instruments such as regulations, strategic plans, presidential decrees, or national digital transformation frameworks.

Level 4: Sparse and Fragmented Recognition

Countries where statutory recognition remains limited, fragmented, or largely absent.

Data collection

The countries covered in this study were assessed against a common analytical framework informed by the G20 Framework for Systems of Digital Public Infrastructure, Digital Public Goods standards, and comparative digital government literature (India G20 Task Force on Digital Public Infrastructure, 2024; OECD, 2024). This study draws upon a diverse set of primary and secondary sources spanning the period 2017–2026. Primary sources included statutory acts, government policy documents, parliamentary records, and official regulatory guidance, providing direct insight into how countries have codified DPI governance (Ministry of Science and ICT, 2025; Australian Government, 2024; Republic of the Philippines, 2025). Secondary sources included academic studies, international organisation reports, and policy briefs that interpreted, analysed, or evaluated DPI legal frameworks, and their implementation (Chaudhuri, 2023; Smith & Russell, 2024).

It is important to note that most sources were in English, which may have limited the visibility of domestic debates or non-English-language legal interpretations, particularly in countries such as South Korea, China, and Indonesia. While Google Translate was utilized to interpret non-English texts, it is important to note that establishing a 'statutory definition' relies heavily on exact legal terminology. Nuanced distinctions between a binding primary statute, a secondary executive decree, or an administrative guideline in jurisdictions like South Korea, China, and Indonesia may not be perfectly captured by automated translation, which limits the definitive classification of their legal frameworks. Besides, availability of sources varied across countries. Nations with transparent, digitised legislative systems, such as Australia and Singapore, were easier to analyze, whereas states affected by conflict or political opacity, including Myanmar and Afghanistan, presented significant gaps in available documentation. These limitations shaped the scope and confidence of comparative analysis.

Findings

The comparative analysis reveals significant variation in how governments across the Asia-Pacific region conceptualise, define, and institutionalise DPI. While digital transformation has become a policy priority in almost every country examined, the legal recognition of DPI remains highly uneven. Most countries have developed legal and regulatory frameworks governing individual components of DPI such as digital identity, digital payments, cybersecurity, data governance, and electronic government services, but relatively few have formally defined DPI as a distinct governance concept.

The defining boundary between Level 2 and Level 3 rests on the role of primary legislation. Malaysia qualifies for Level 2 because its policy initiatives (like MyDIGITAL and PADU) are anchored by hard primary statutes, such as the Communications and Multimedia Act 1998 and the Personal Data Protection Act 2010. Conversely, Indonesia is classified as Level 3 because its SPBE framework and digital integration efforts are primarily driven by executive action, specifically Presidential Regulation No. 82/2023, rather than a consolidated base of primary parliamentary legislation

Table 1: Classification of country based on their legal and policy framework on DPI definition

Country	Classifi-cation	Key Legal / Policy Basis	Key Observation
South Korea	Level 1	Framework Act on Intelligent Informatization	Strong statutory architecture supporting digital transformation and public digital infrastructure.
Australia	Level 1	Digital ID Act 2024	Comprehensive legal governance of digital identity with strong accountability mechanisms.
India	Level 1	G20 Task Force on DPI; Aadhaar; UPI ecosystem	One of the few countries with an explicit and comprehensive official DPI definition.
Papua New Guinea	Level 1	Digital Government Act 2022	Explicit statutory recognition of digital infrastructure and digital government systems.

Singapore	Level 2	PDPA, Cybersecurity Act, Smart Nation framework	Highly advanced DPI ecosystem without a dedicated DPI definition.
Malaysia	Level 2	PDPA 2010, CMA 1998, MyDIGITAL, PADU, MyDigital ID	Strong sectoral foundations but fragmented governance and no formal DPI definition.
Philippines	Level 2	PhilSys Act, E-Governance Act 2025	Increasing integration of digital government systems.
Pakistan	Level 2	Digital Nation Pakistan Act 2025, NADRA, Raast	Moving towards integrated digital infrastructure governance.
China	Level 3	Digital China Strategy, New Infrastructure Agenda	Extensive policy recognition but limited statutory definition.
Indonesia	Level 3	Presidential Regulation No. 82/2023	Executive-led integration of digital government services.
Bangladesh	Level 3	Smart Bangladesh 2041, Cyber Security Act 2023	Policy-driven digital transformation agenda.
Myanmar	Level 3	E-Government Master Plan, Cybersecurity Law	Digital governance constrained by political instability.
Nepal	Level 4	Digital Nepal Framework	Fragmented legal recognition and institutional arrangements.
Afghanistan	Level 4	Various digital governance initiatives	Limited legal recognition and institutional capacity.

Cluster 1: Advanced Recognition and Formal Definition

South Korea, Australia, India, and Papua New Guinea demonstrate the strongest levels of formal recognition of DPI concepts, although they have arrived at this position through different legal and institutional pathways.

South Korea represents one of the most mature examples of statutory institutionalisation in the region, illustrating how DPI definitions can be embedded within an all encompassing digital governance code. Instead of enacting a narrow or standalone act specifically named for DPI, South Korea legally defines its core digital components within the Framework Act on Intelligent Informatization (Government of the Republic of Korea, 2020). The Act establishes a comprehensive legal architecture supporting digital transformation, information infrastructure, data utilisation, digital government services, and public-sector innovation. It legally codifies the foundational building blocks of the digital state by defining hyper connected intelligent IC infrastructure as “a hyper connected intelligent IC network, and devices, facilities, software, data, etc. related to information communications and intelligent information technology, which are used as connected to such network”. This comprehensive legal definition ensures that all subsequent technologies, from public data registries to cloud computing networks, fall under a single, unified statutory definition and regulatory authority. This expansive definition is a product of a long standing legislative evolution, tracing back from the Framework Act on National Informatization in 2009 to its current amended form in 2020, establishing a permanent and legally binding state asset model.

In stark contrast to the highly centralised and state-directed model of South Korea, Australia adopts a more targeted, decentralised approach. Rather than enacting an overarching and all-encompassing digital infrastructure code, Australia utilises the Digital ID Act 2024 to focus primarily on digital identity as the foundational identity layer of its wider DPI by establishing an economy-wide accreditation scheme (Australian Government, 2024). Australia's model demonstrates how strong statutory recognition can emerge through sector-specific legislation without requiring a dedicated DPI law. Instead of defining a centralised state database, the Australian Act legally defines and regulates interactive, federated network roles. It codifies the definitions of an Identity Service Provider (an entity that generates, manages, maintains, or verifies identity information) and an Attribute Service Provider (an entity that verifies specific claims or attributes about an individual, such as age or professional credentials). By restricting its statutory definitions to these federated roles, the Australian model demonstrates how strong legal recognition can emerge through precise, sector specific legislation that regulates a distributed marketplace rather than mandating a unified, state run digital infrastructure.

India occupies a unique position within the region. Unlike Australia or South Korea, the definition of DPI is not codified under a specific act or primary statute. However, India warrants Level 1 classification because the Report of India's G20 Task Force on Digital Public Infrastructure (India G20 Task Force on Digital Public Infrastructure, 2024), published by the Department of Economic Affairs, functions as a highly authoritative administrative framework. It provides an explicit, comprehensive official conceptualisation of DPI (encompassing identity, payments, and

data exchange) that actively directs the domestic ecosystem, operating with the de facto weight of statutory recognition. Therefore, its definition can be considered an official government position.

Papua New Guinea presents an emerging example of Level 1 statutory recognition where the legal definition of digital infrastructure is explicitly codified in primary law. The Digital Government Act 2022 serves as the authoritative legal framework, providing clear statutory boundaries that govern the national digital stack. (Government of Papua New Guinea, 2022). Section 2 of the Act defines digital infrastructure with immense granularity as “any device or mechanism used to or capable of delivering data and digital services, and may be physical or virtual, or hardware or software”. This definition is highly significant because it explicitly lists cloud computing infrastructure, national data repositories, application programming interfaces (APIs), and the Government Private Network within its legal scope. By enacting this highly detailed definition, the statute eliminates legal ambiguity regarding what constitutes public digital property, granting the Department of Information and Communications Technology the explicit regulatory mandate to govern these systems. While technical systems such as the SevisPNG portal and SevisPass identity scheme have been launched, the statutory framework remains focused on defining the physical and virtual rails of government technology, leaving the separate legal definitions of personal data protection to pending draft legislation (Department of Information and Communications Technology, 2025).

In summary, these countries demonstrate the strongest levels of legal clarity concerning the legal definition of DPI.

Cluster 2: Composite Statutory Frameworks

Singapore, Malaysia, the Philippines, and Pakistan possess substantial legal foundations supporting DPI despite lacking comprehensive formal definitions equivalent to India's framework.

Singapore arguably operates one of the most advanced digital ecosystems in the Asia-Pacific region. However, rather than defining DPI as a singular legal concept, Singapore governs its digital infrastructure through an interconnected network of legislation and institutions. The Personal Data Protection Act 2012, Cybersecurity Act 2018, Public Sector Governance Act 2018, Electronic Transactions Act, and various Smart Nation initiatives collectively provide the legal and institutional foundations for platforms such as Singpass, MyInfo, and PayNow (Smart Nation and Digital Government Group., 2018; World Bank, 2022). This distributed legal model is exemplified by how Singapore defines and regulates public sector data sharing. Because the Personal Data Protection Act 2012 originally excluded government agencies from its data protection rules, Singapore enacted the Public Sector (Governance) Act 2018 to establish a distinct, parallel statutory definition for public sector data management. This Act legally defines the boundaries of data sharing among government departments, prescribing strict statutory definitions for the secure transfer, storage, and access of citizen information across public systems. Singapore’s experience demonstrates that highly integrated DPI systems can achieve

legal coherence through coordinated, composite statutes and robust institutional frameworks, proving that a single, unified "DPI Act" is not a prerequisite for statutory maturity. In practice, Singapore demonstrates that highly integrated DPI ecosystems can emerge through strong institutional coordination even without a dedicated statutory definition. The Singaporean experience suggests that governance coherence may be as important as formal legal definitions in enabling effective digital transformation.

Malaysia governs its digital public infrastructure through a sectoral and policy-led model, guided by the MyDIGITAL Blueprint and anchored by existing statutes such as the Communications and Multimedia Act 1998 and the Personal Data Protection Act 2010 (Economic Planning Unit, 2021; Ministry of Economics, 2024). (Economic Planning Unit, 2021). Under this fragmented framework, the national digital identity platform, MyDigital ID, lacks a standalone primary statute. It is defined in policy instruments as a secure, integrated platform for identity verification and data sharing to enhance digital services, privacy, and cybersecurity. Because there is no dedicated primary legislation to define its scope, MyDigital ID is governed by the executive branch without statutory provisions defining public oversight, independent regulatory bodies, or transparent citizen redress mechanisms. Furthermore, because the Personal Data Protection Act 2010 explicitly excludes federal and state governments from its legal definitions of data privacy, the administrative data exchange layers of Malaysia's public sector operate without a statutory definition of government data liability, illustrating the limitations of a policy led, non statutory approach to DPI definition. The absence of a dedicated legal definition of DPI means that governance remains dispersed across multiple ministries, agencies, and policy domains. Malaysia therefore represents a case where implementation initiatives are evolving more rapidly than legal conceptualisation. Recent developments surrounding digital identity, integrated databases, and government service digitisation suggest movement towards a more coordinated framework, although statutory consolidation remains limited.

The Philippines demonstrates a highly structured approach to digital public infrastructure, using primary legislation to define both identity and administrative digital assets. This legal foundation is anchored by Republic Act No. 11055 (the Philippine Identification System Act 2018) and the E Governance Act of 2025. (Government of the Phillipines, 2018, 2025). The E Governance Act of 2025 introduces a powerful statutory definition for public sector technology, defining ICT Assets as “any data, device, equipment, infrastructure, system, or component thereof, utilized to ensure or support the proper and efficient operation and implementation of ICT related programs and delivery of ICT services”. This statutory definition is legally tied to a mandated "consolidated process architecture," which legally requires government agencies to adopt open, interoperable standards. By defining ICT assets in this manner, the Philippines’ statutory framework establishes a clear legal basis for the adoption of open source Digital Public Goods (DPGs), such as the Modular Open Source Identity Platform (MOSIP), creating a legally enforceable requirement for system interoperability and public auditability across the state's digital infrastructure. These developments indicate increasing recognition of the need for integrated digital government services and interoperable systems. Nevertheless, legal frameworks continue to focus primarily on individual systems rather than DPI as a coherent

governance concept. The Philippines therefore occupies an intermediate position between sectoral governance and more integrated approaches.

Pakistan's Digital Nation Pakistan Act 2025 represents one of the most ambitious legislative efforts within this cluster. Combined with the National Database and Registration Authority (NADRA), the Raast instant payment system, and broader digital government initiatives, Pakistan is gradually developing a more integrated governance architecture (Government of Pakistan, 2025). The Digital Nation Pakistan Act 2025 establishes an explicit, three tier statutory definition for its national digital systems, legally defining the "Pakistan Stack" as an integrated digital infrastructure comprising identity, payments, and data exchange. However, the legal boundaries of this definition are severely constrained by Section 29 of the Digital Nation Pakistan Act 2025, which functions as a statutory ouster clause. Section 29 explicitly dictates that no decision, order, or action taken under the Act “shall be questioned by any agency or challenged in any court or tribunal”, and legally prohibits any court from granting an injunction against the operations of the Pakistan Digital Authority. This clause legally redefines the relationship between the state and the citizen, removing judicial oversight from the very statute that defines the national data exchange layer. Consequently, while Pakistan possesses a highly advanced statutory definition of DPI on paper, the law simultaneously defines the state's administrative power as entirely immune to judicial review, rendering statutory citizen redress non-existent.

A defining feature of this cluster is that legal foundations exist across multiple domains, but they remain dispersed across separate statutes and institutions. DPI emerges as a functional outcome of governance arrangements rather than as an explicitly recognised legal category. These countries demonstrate that substantial digital infrastructure can be developed through composite legal frameworks, although such approaches may face challenges relating to coordination, accountability, and long-term governance coherence.

Cluster 3: Executive and Policy-Led Recognition

China, Indonesia, Bangladesh, and Myanmar primarily recognise DPI through executive instruments, strategic plans, and national development frameworks rather than comprehensive legislation.

China's approach is particularly significant because of its scale, state capacity, and global influence. Through initiatives such as Digital China, the New Infrastructure agenda, and successive Five-Year Plans, China has developed one of the world's most ambitious digital transformation programmes (Central Committee of the Communist Party of China & The State Council of the People's Republic of China, 2023). China’s legal definition of digital public infrastructure is codified through the concept of "New Infrastructure" (Xin Jichu), formalized under national policy plans and directed by the National Development and Reform Commission. The state legally divides this infrastructure into three distinct categories: Information Infrastructure (defining 5G networks, the Internet of Things, and blockchain), Integrated Infrastructure (defining the digital transformation of traditional physical networks), and

Innovation Infrastructure (defining public research and development systems). This highly structured administrative definition is supported by an underlying statutory base comprising the Cybersecurity Law 2017, the Data Security Law 2021, and the Personal Information Protection Law 2021, which collectively define the state's final authority over all domestic digital assets. . However, the concept of DPI itself remains embedded primarily within planning frameworks and administrative strategies rather than a dedicated statutory definition. China's approach reflects a governance tradition in which state planning and executive coordination often play a more prominent role than legislative codification.

Indonesia follows a decree-led pathway and relies heavily on Presidential Regulation No. 82 of 2023 and the Electronic-Based Government System (SPBE) framework. These instruments seek to coordinate digital transformation across government agencies and establish common digital platforms for public services (Government of Indonesia, 2023). This executive regulation defines the legal framework for the Electronic Based Government System (SPBE) and mandates the creation of INA Digital. Under this decree, the state defines three core digital services: INA Ku (the public services portal), INA Pas (the national digital identity), and INA Gov (the internal administrative collaboration system). However, because these definitions are established via a presidential regulation rather than binding primary legislation, they lack the statutory permanence of a parliamentary act, leading to weak enforcement of data interoperability definitions across provincial and municipal jurisdictions. Indonesia's model reflects a pragmatic effort to achieve integration through executive leadership rather than legislative consolidation. While this approach provides flexibility and allows rapid policy adaptation, it may also create uncertainties regarding institutional accountability and legal permanence.

Bangladesh demonstrates a transition from policy-led definitions to statutory frameworks. Its Smart Bangladesh 2041 vision similarly illustrates how governments can articulate ambitious digital transformation agendas through strategic planning frameworks (Aspire to Innovate, 2022). The initiative seeks to transform Bangladesh into a knowledge-based and technology-driven economy supported by digital infrastructure, innovation ecosystems, and public service digitisation. To establish a firmer legal basis, the state enacted the Personal Data Protection Ordinance (PDPO) on 6 November 2025 (placed on a parliamentary statutory footing in April 2026). This statute introduces the first formal legal definitions for a national data governance authority and defines the legal boundaries of public data registries. However, because the enforcement of these statutory definitions is legally phased out to 2027, the legal boundaries of Bangladesh's data infrastructure remain in a transitional phase. However, while legal recognition exists through cybersecurity and ICT legislation, the broader governance architecture remains heavily dependent upon policy frameworks and executive direction rather than comprehensive statutory foundations.

Myanmar presents a more challenging case. It illustrates a different legal divergence, where the official definitions of digital systems serve to codify executive dominance. The official e Governance Master Plan 2030 defines digital public systems purely as instruments of administrative modernization and state efficiency. Under the military State Administration

Council, this definition is legally enforced by the 2025 Cybersecurity Law, which defines the state's unrestricted right to access user data while criminalizing tools that protect digital privacy, such as virtual private networks. Although digital governance plans, cybersecurity regulations, and e-government initiatives exist (State Administration Council, 2025; World Bank, 2026), political instability has significantly constrained institutional development and legal certainty (Hoffman & Feldstein, 2026). Because the official state definitions exclude citizen safeguards, civil society organizations have developed a defensive, legal conceptual counter model known as Public Interest Infrastructure. This model defines digital public systems as a set of digital tools and spaces that must legally and intentionally serve the public interest and digital rights, rather than state or commercial surveillance. This counter definition argues that digital infrastructure must be legally defined by user centric data governance and decentralised access, creating a conceptual blueprint to challenge state dominated legal definitions that compromise human rights. As a result, DPI-related governance remains fragmented and difficult to assess comprehensively. The Myanmar case demonstrates how political and institutional conditions can affect the development of digital governance regardless of technological aspirations.

This cluster highlights an important regional trend: many governments continue to rely on executive leadership, strategic planning, and administrative coordination to drive digital transformation. Such approaches may facilitate rapid implementation but often provide weaker legal foundations than comprehensive statutory frameworks.

Cluster 4: Sparse and Fragmented Recognition

Nepal and Afghanistan exhibit the weakest levels of statutory recognition among the fourteen countries reviewed.

In Nepal, there is a complete absence of a unified, primary statutory definition for digital public infrastructure. Digital governance initiatives remain dispersed across multiple policies, regulations, and development programmes. Efforts have been made to promote digital identity systems, electronic government services, and broader digital transformation through initiatives such as the Digital Nepal Framework 1.0 and 2.0 (Ministry of Communication and Information Technology, 2019, 2025). However, there is limited evidence of a coherent legal architecture explicitly recognising DPI as an integrated governance concept. Existing arrangements remain fragmented across sectors and institutions, limiting overall coherence. The legal definitions of cybersecurity, data liability, and infrastructure standards remain undefined in primary law due to the perpetual stalling of the Information Technology and Cyber Security Bill in parliament. This lack of a statutory definition for infrastructure security and system redundancy was highlighted during a major technical outage in 2025, when a single vulnerability in the centralized Government Integrated Data Center (GIDC) paralyzed digital systems nationwide. Because the law fails to define cybersecurity requirements or administrative liability for public databases, Nepal's digital stack operates in a state of statutory fragmentation where data registries lack legal protection.

Afghanistan faces even greater challenges. Political instability, institutional fragmentation, limited administrative capacity, and infrastructure constraints have hindered the development of comprehensive digital governance frameworks (Shires & Wilkinson, 2024). Existing digital initiatives remain fragmented and often depend on external support or donor-driven projects. Afghanistan represents a complete statutory vacuum where pre-existing digital governance laws have been rendered entirely defunct under the De Facto Authorities (the Taliban). The state possesses a highly sophisticated, biometric linked digital identity database (the Tazkira system) originally built under international development frameworks. However, in the absence of any data privacy laws, independent regulatory oversight, or statutory definitions of citizen rights, the legal definition of the Tazkira has been completely repurposed. Under current de facto decrees, the Tazkira is defined not as a tool for public service inclusion, but as an administrative instrument for state surveillance and population tracking. Crucially, because there are no statutory safeguards defining universal access, approximately 40% of the population (disproportionately consisting of women, girls, and marginalized groups) are legally and administratively excluded from obtaining a biometric Tazkira, which under de facto decrees denies them the legal right to access cellular services, banking, and basic public administration. While digital governance aspirations exist, statutory recognition of foundational digital infrastructure remains limited. Consequently, Afghanistan represents the least developed statutory environment among the jurisdictions examined.

The experiences of Nepal and Afghanistan illustrate that digital transformation requires more than technological investment alone. Institutional capacity, governance stability, and legal frameworks remain essential prerequisites for sustainable digital development.

Regional Patterns and Emerging Trends

Several broader patterns emerge from the comparative analysis:

1. Explicit statutory definitions of DPI remain rare across the Asia-Pacific region. Most governments regulate the constituent components of DPI, such as digital identity, digital payments, cybersecurity, interoperability, and data governance, rather than DPI itself. India therefore represents an important exception through its G20 Task Force framework, which provides one of the most comprehensive official conceptualisations currently available (India G20 Task Force on Digital Public Infrastructure, 2024);

2. There is evidence of growing convergence around core governance principles. Across different political systems and legal traditions, governments increasingly emphasise interoperability, inclusion, cybersecurity, privacy protection, accountability, and digital identity as foundational elements of digital governance. This suggests that while legal frameworks may differ, underlying governance objectives are becoming increasingly aligned;

3. Statutory maturity appears closely associated with broader state capacity and digital governance development. Countries with established traditions of e-government, stronger

institutions, and higher administrative capacity generally exhibit more coherent legal frameworks. South Korea, Singapore, and Australia illustrate this pattern particularly clearly;

4. Legal recognition frequently lags behind technological deployment. Many governments have already implemented sophisticated digital systems before developing comprehensive legal frameworks governing them. This pattern is particularly evident in countries where policy innovation and technological implementation have advanced more rapidly than legislative reform; and

5. International norm-setting processes are becoming increasingly influential. India's G20-led DPI framework, the work of international organisations such as the World Bank and UNDP, and growing cross-border cooperation suggest that future statutory approaches may become more aligned around shared governance principles. Rather than converging on a single legal model, countries appear to be converging on a common set of objectives and values underpinning DPI governance.

These findings suggest that the future development of DPI governance in the Asia-Pacific region is likely to involve a gradual movement towards greater legal clarity, stronger interoperability frameworks, and enhanced institutional coordination. However, significant variation is likely to remain due to differences in political systems, legal traditions, governance capacities, and developmental priorities.

Limitations

This analysis represents a broad regional comparison rather than a comprehensive legal assessment of DPI governance across the Asia-Pacific region. The limitations are as below:

1. The nature of the evidence base on DPI is fragmented and budding. DPI remains a relatively recent policy concept, and many DPI initiatives are still under development. Consequently, long-term evaluations of statutory effectiveness remain limited, and evidence across jurisdictions is uneven (UNDP, 2023);

2. Data availability and transparency remain an issue. The analysis relies heavily on publicly available government documents, policy reports, and secondary literature. In many jurisdictions, legal and regulatory information is dispersed across multiple agencies, published inconsistently, or difficult to access. Differences in transparency standards also affect the reliability and comparability of available evidence. There are also risks of overlooking the actual developments due to different language use, inaccurate keywords, lack of familiarity over the primary and secondary sources, and undocumented progress;

3. There is a significant lack of disaggregated implementation data. While legal frameworks can often be identified and analysed, publicly available information rarely provides sufficient detail to assess how statutory provisions affect different demographic groups or whether digital systems operate equitably in practice;

4. Definitional ambiguity of DPI remains a challenge. Governments frequently use different terminology, including digital government, digital transformation, intelligent informatisation, national digital infrastructure, and electronic governance, to describe functionally similar systems. These differences create difficulties in establishing direct comparisons across jurisdictions (OECD, 2024);

5. Some of the most important objectives associated with DPI definition, including public trust, institutional capacity, digital sovereignty, and state legitimacy, are ecosystem-level effects that emerge over long periods of time and cannot be adequately reflected through statutory definition alone (World Bank, 2024); and

6. Technological development often exceeds the pace of legislative reform. Emerging technologies such as artificial intelligence, cloud computing, and advanced data ecosystems continue to evolve faster than legal definitions and frameworks can adapt. Consequently, statutory definitions may not always reflect contemporary technological realities.

3. Who Oversees DPI and On What Legal Authority? Legal Foundations and Oversight Bodies Across the Asia-Pacific

By Manas Joshi

Background and literature

Discussion of how Digital Public Infrastructure should be overseen and on what legal foundation, has expanded substantially since the G20 New Delhi Leaders' Declaration of 2023, which framed DPI as "a set of shared digital systems that should be secure and interoperable and can be built on open standards and specifications" (India G20 Task Force on DPI, 2024). The Global Digital Compact, adopted at the UN Summit of the Future in 2024, took the conversation further and acknowledged "digital public goods and digital public infrastructure to be key drivers of inclusive digital transformation and innovation" (United Nations General Assembly, 2024). Across the literature that follows from these documents, however, the questions of who oversees DPI and what legal authority underpins it have received markedly less comparative attention than the question of what DPI is for. These two governance dimensions are the focus of this study.

A first thread in the existing conversation concerns why consolidated oversight matters at all. International organisations have argued that DPI, because it touches identity, payments and data flows at population scale, requires institutional arrangements capable of coordinating across sectoral regulators, central banks, identity agencies and data-protection authorities. The World Bank Group treats coordinated oversight as a precondition for the trust and accountability that make population-scale DPI viable (World Bank, 2025a). The UNDP frames enabling governance, alongside open technology standards and a competitive market, as one of three pillars of effective DPI (UNDP, 2023). The OECD's review of South Korea's digital government illustrates the centralised-coordination model in practice, with the Ministry of the Interior and Safety, the Ministry of Science and ICT and the Presidential Committee on the Digital Platform Government operating in concert on a settled statutory base (OECD, 2025a). The competing view, articulated most clearly through Indian and Brazilian experience and synthesised by Eaves and Rao (2025), favours federated arrangements in large, plural and decentralised states. The comparative literature is generally cautious about prescribing a single model, recognising that what works in a small unitary state is unlikely to fit an archipelago of 270 million.

A second thread concerns what kind of legal foundation produces functional DPI. Sarjito and Thamrin (2026) demonstrate, through their Indonesia and Estonia comparison, that policy-led frameworks such as Indonesia's SPBE routinely underperform statute-led foundations on enforceability and interoperability, even when institutional architecture is broadly similar. The CAICT (2025) report presents an alternative party-state perspective in which a strong policy overlay, namely the 2023 Overall Layout Plan for the Construction of Digital China, directs an

underlying statutory base comprising the Cybersecurity Law of 2017, the Data Security Law of 2021 and the Personal Information Protection Law of 2021. Kapur and LaForge (2026), writing for the Digital Public Goods Alliance, takes a third position. They argue that legal foundations matter less than the openness of the underlying technical stack, with the Philippines featured as one of three country case studies on how DPG-recognised infrastructure can be deployed within existing statutory regimes. Across these positions, the recurring point of agreement is that statutory grounding tends to translate into stronger accountability outcomes, even when the precise design varies.

Comparative experience both within and beyond APAC informs the analysis. The European Union's General Data Protection Regulation has become the de facto global reference point for data-protection statutes and its pairing with independent national data-protection authorities offers a baseline against which APAC arrangements can be assessed (European Parliament and Council, 2016). Within APAC, Singapore's whole-of-government digital infrastructure, operationalised by GovTech Singapore under settled legislation including the Personal Data Protection Act 2012 and the Public Sector (Governance) Act 2018, illustrates what Sarjito and Thamrin (2026) treat as institutional coherence paired with legal interoperability (GovTech Singapore, 2022). India's federated architecture, in which UPI sits under the Reserve Bank of India, Aadhaar under UIDAI and the DPDP regime under MeitY and the Data Protection Board of India, is documented in IIM Bangalore and Protean's State of DPI in India (2025). Unlike Singapore's centralised whole-of-government model, India's approach distributes authority across multiple sectoral institutions while maintaining interoperability across the digital public infrastructure stack. It offers a substantially different institutional pathway that has nevertheless produced rapid scale. Each of these comparisons is partial. None maps directly onto the full diversity of APAC institutional and legal arrangements that this analysis examines.

Why does this matter for how DPI serves people? DPI handles foundational identity, payments and data flows for entire populations. The question of who oversees it and on what legal authority directly determines whether citizens can challenge wrongful decisions, whether breaches trigger meaningful enforcement and whether interoperability standards are enforceable against agencies. Where the governance and legal foundations are weak, the technical infrastructure can be deployed at scale without commensurate accountability. This pattern recurs across multiple APAC cases in the country observations that follow.

Definition and baseline in this study

For the purposes of this study, Digital Public Infrastructure (DPI) refers to the set of foundational, society-scale digital systems that enable citizens, businesses and government to interact and transact online. These typically include digital identity, digital payments and data-exchange platforms, supported by physical infrastructure and an enabling governance and legal framework. The definition draws on the G20 Task Force framework (India G20 Task Force on DPI, 2024) and the Global Digital Compact (United Nations General Assembly, 2024). It is consistent with the operational definitions used by the World Bank Group, UNDP, OECD and the Digital Cooperation Organization.

1. Consolidated Oversight Body

This dimension captures the institutional architecture overseeing DPI. It asks which bodies hold authority over which layers of the stack, whether a single consolidated regulator exists and how independence and coordination are configured. The dimension is coded on a four-tier typology with a functional flag.

Code	Description
T1	Single consolidated body with cross-stack DPI authority
T2	Lead agency plus sectoral regulators
T3	Inter-agency committee or coordination mechanism
T4	Decentralised, fragmented or no body designated

Each cell is additionally flagged Nominal (the body exists on paper) or Operational (the body functions in practice with operational independence).

2. Legal or Regulatory Foundation

This dimension captures the body of binding legal instruments that authorise, govern and constrain DPI. This includes primary legislation, subordinate regulation and, where these are absent, the executive or policy instruments operating in their place. The dimension is coded on a parallel four-tier typology.

Code	Description
L1	Dedicated DPI statute (a single comprehensive primary law)
L2	Composite statutory base (multiple primary laws together form the foundation, with no single DPI law)
L3	Policy/decree-led (DPI rests primarily on executive instruments)
L4	Minimal/absent (no comprehensive legal foundation)

A separate Nominal/Operational assessment distinguishes between legal instruments that exist on paper and those that operate effectively in practice, including whether judicial review is available, whether a data-protection authority is operational and whether interoperability frameworks have legal force.

Three considerations in shaping the typologies

1. The typologies are descriptive rather than normative. They classify variation in arrangement without presupposing that any particular model, whether centralised, federated, or sectoral, is intrinsically superior.
2. The typologies are designed to be paired. A body in T is established or empowered by an instrument in L and the strongest comparative readings emerge when the two are read together.
3. The Nominal/Operational flags acknowledge a recurring finding in the existing literature (Sarjito & Thamrin, 2026; Shires & Wilkinson, 2024) that institutional and legal architecture on paper frequently diverges from how arrangements operate in practice.

Data collection

For the governance and legal-foundation columns, a three-source triangulation rule was applied where possible. The rule combines:

1. A government primary source documenting the formal architecture,
2. A peer-reviewed or institutional analysis assessing effectiveness and
3. A civil society or independent journalism documenting operational harms.

Three significant mid-research corrections illustrate the value of this rule. The below examples justify the same as above:

a. The original China entry, drafted from civil society sources alone, materially under-described the institutional architecture. Only the CAICT (2025) report revealed the National Data Administration's central role.
b. The Indonesia entry, drafted from government press releases, materially overstated the framework's enforceability. Only Sarjito and Thamrin (2026) revealed the explicitly non-binding character of the SPBE framework.
c. The Pakistan entry, initially coded based on the existence of the Digital Nation Act, required correction after an annotated review of the Act revealed Section 29's ouster of judicial review.

Findings

Finding 1. The single most pervasive gap is operational data protection. Across the fourteen countries, only South Korea, Singapore, the Philippines and Australia pair a comprehensive data-protection statute with an operating independent authority. India brought the DPDP Act into force and constituted the Data Protection Board of India on 13 November 2025; the Board is currently being operationalized, with member appointments underway (MeitY, 2026). Pakistan's data-protection bill has progressed to a 2025 draft but has not been enacted and its proposed National Commission for Personal Data Protection is not yet operational (ICLG, 2025). Bangladesh enacted the Personal Data Protection Ordinance on 6 November 2025,

subsequently placed on a parliamentary statutory footing in April 2026, which establishes a national data governance authority. This authority is not yet operational and enforcement is phased toward 2027 (DCO, 2025). Indonesia's Personal Data Protection Authority is mandated by the 2022 PDP Law and is the subject of a draft Presidential Regulation published in February 2026, but it is not yet operational. Papua New Guinea's National Data Protection and Governance Policy remains in draft (DICT, 2025). Nepal's Personal Data Protection Bill is pending. Myanmar and Afghanistan have no such legislation. This finding tracks almost exactly onto the cluster structure. Cluster A countries have operational DPAs and all other clusters do not.

Finding 2. Form and function diverge in a minority of high-stakes cases. Pakistan provides the sharpest case. It has the most explicit dedicated DPI statute in the set (the Digital Nation Pakistan Act 2025, Act No. I of 2025). Yet Section 29 of that Act expressly provides that no decision of the Pakistan Digital Authority "shall be questioned by any agency or challenged in any court or tribunal", an ouster clause that removes judicial review as a check on the primary DPI statute itself (Digital Nation Pakistan Act, 2025, s.29). Myanmar offers a parallel case from a different starting point. The e-Governance Master Plan 2030 establishes an elaborate two-tier committee structure with eight specialised subcommittees, but the entire architecture operates under the State Administration Council without independent civilian oversight (Ministry of Transport and Communications [Myanmar], 2024). Indonesia presents a third variant. The SPBE framework operates through Presidential Regulation No. 82/2023 but is characterised by peer-reviewed analysis as "non-binding" with "weak enforcement of interoperability standards" (Sarjito & Thamrin, 2026). In all three cases, substantial legal and institutional frameworks exist. However, operational safeguards, accountability mechanisms and enforceable protections remain limited.

Finding 3. Singapore and Malaysia provide a natural experiment in statutory design. Both countries' principal data-protection statutes, Singapore's Personal Data Protection Act 2012 and Malaysia's Personal Data Protection Act 2010, expressly exclude public agencies from the data-protection regime that applies to the private sector. Singapore closed that carve-out deliberately through the Public Sector (Governance) Act 2018, which governs data sharing across government agencies. Although public agencies remain outside the Personal Data Protection Act itself, the Public Sector (Governance) Act 2018 brings Singapore's government-operated DPI within a comprehensive statutory framework. The result is that Singapore's government-operated DPI sits inside a complete statutory regime (Attorney-General's Chambers, Singapore, 2018). Malaysia has left the carve-out open. Under the 13th Malaysia Plan, the government has proposed establishing a National Data Commission to address this gap (Ministry of Digital, Malaysia, 2025). The two countries reached the same statutory starting point but resolved it in opposite ways. This illustrates that the existence of a data-protection statute alone is not determinative. What matters is whether government-operated DPI is subject to enforceable statutory safeguards and accountability mechanisms.

Finding 4. The Philippines is the most legislatively grounded country in the set. Three primary statutes anchor the foundation: Republic Act No. 11055 (Philippine Identification System Act, 2018), Republic Act No. 10173 (Data Privacy Act of 2012) and the E-Governance Act of 2025. The Data Privacy Act of 2012 established the National Privacy Commission as an independent authority with jurisdiction over both public and private sectors. On this statutory base, the Philippines has built one of the most distinctive DPI implementations in APAC, drawing on open-source Digital Public Goods. These include MOSIP for digital identity, Mojaloop for payments interoperability, OpenG2P for government-to-person transfers and OpenSPP for social protection. The deployment proceeds within an explicit national strategy of phased, modular rollout (Kapur & LaForge, 2026). The combination of mature legal infrastructure and DPG-based technical choices distinguishes the Philippines from both the centralized-proprietary cluster (Singapore, Malaysia) and the policy-led developing cases.

Finding 5. Political-system type correlates with foundation type. Democratic systems with mature legislative institutions, namely South Korea, Singapore, Philippines, Australia and India, cluster at L2 with composite statutory bases. Policy-led developing democracies (Indonesia, Bangladesh, Papua New Guinea) cluster at L3, where presidential regulations, ministerial directives and national master plans substitute for primary legislation. Myanmar, under a military administration, clusters at L3 while China sits at L2 under a strong party-state policy overlay. Afghanistan under the De Facto Authorities sits at L4. The correlation is not deterministic. Pakistan, formally democratic, sits at L1. The broad alignment nevertheless suggests that legislative depth on DPI tracks broader institutional depth.

Finding 6. The most consequential recent shift in the set is India's DPDP Act activation. On 13 November 2025, the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Act 2023 and its accompanying Rules 2025. Provisions establishing the Data Protection Board of India took effect immediately, with consent-manager and remaining provisions phased in through 2026 to 2027 (Ministry of Electronics and Information Technology [MeitY], 2023; MeitY, 2025). This moves India from a "statute-in-place, board-not-active" status, which had held throughout the early research period, to a "statute-in-force, authority constituted and being operationalized" status, moving it toward the Cluster A profile as the Board is stood up.

Finding 7. DPI deployment is outpacing statutory privacy infrastructure in several countries. Papua New Guinea's SevisPNG ecosystem was formally launched on 24 November 2025, but the country has no comprehensive Data Protection Act in force. DICT's National Data Protection and Governance Policy remains in draft (DICT [PNG], 2025). Bangladesh's a2i has deployed the ekShop platform as a recognised Digital Public Good for digital commerce (DCO, 2025), while the national data governance authority established by the November 2025 ordinance is not yet operational (Government of Bangladesh, 2025). Indonesia's PDP Law was enacted in 2022 but is described in peer-reviewed analysis as "a step forward but under-implemented" with no operational authority (Sarjito & Thamrin, 2026). The pattern is consistent. Technical deployment is ahead of the legal and institutional accountability layer, often by years.

Finding 8. Cross-border integration is emerging in payments but not in identity. The clearest cross-border DPI development in the set is in payments. Nepal's National Payment Interface is being integrated with India's Unified Payments Interface to enable seamless cross-border QR payments (Nepal Rastra Bank, 2025). The Philippines is deploying Mojaloop for similar purposes. No equivalent cross-border identity recognition has emerged within APAC and the legal architecture for it does not yet exist in any country in the set. This is consistent with the broader finding that statutory foundations are stronger in the payments layer, where central banks operate under long-established financial-regulation statutes, than in the identity and data-exchange layers, where the legal foundations are more recent and less consolidated.

Single most important takeaway

The headline comparative finding from this study is that statutory form and functional protection broadly track one another across APAC DPI governance but diverge sharply in a minority of consequential cases. The strongest legal foundations do not always produce the strongest accountability. Pakistan illustrates this distinction sharply. The most ambitious DPI rollouts often outpace their statutory privacy regimes. Papua New Guinea, Bangladesh and Indonesia illustrate this pattern. Governance quality across the fourteen countries depends less on whether a statute exists. The cluster structure that emerges from these findings is, accordingly, defined less by the presence or absence of laws and more by the alignment of legal frameworks with operational institutional safeguards.

Aggregating the country observations produces the following distribution:

Country	Legal Foundation (L)	Oversight Body (T)	Cluster
Singapore	L2 (composite, PSGA closes the PDPA carve-out)	T2-Operational	A
South Korea	L2 (composite)	T2-Operational	A
Australia	L2 (composite, dedicated Digital ID Act 2024)	T2-Operational	A
India	L2 (composite, DPDP Act activated 13 Nov 2025)	T2-Nominal (Board constituted; operationalization underway)	B
Philippines	L2 (composite, most legislatively grounded)	T2-Nominal (sectoral, DPG-based)	B
China	L2 (composite under party-state policy overlay)	T2-Nominal (functions but not independent)	B

Malaysia	L2 (PDPA government carve-out left open)	T2-Nominal	B
Pakistan	L1 (form-only, ouster of judicial review)	T2-Nominal	C
Indonesia	L3 (Perpres-led, non-binding SPBE)	T2-Nominal	D
Bangladesh	L3 (PDPO enacted Nov 2025, executive-dominated)	T2-Nominal (authority established, not operational)	D
Papua New Guinea	L3 (Digital Government Act 2022 plus draft DP policy)	T2-Nominal	D
Myanmar	L3 (Master Plan 2030 plus 2025 Cyber Security Law)	T3-Nominal	D
Nepal	L4 (fragmented, key bills pending)	T4-Nominal	E
Afghanistan	L4 (minimal or absent under DFA)	T4-Nominal	E

Reading across both dimensions, the fourteen countries fall into five clusters:

Cluster	Description	Countries
A	L2, T2-Operational: Coordinated and statutorily complete	Singapore, South Korea, Australia
B	L2, T2-Nominal: Coordinated with statutory gap or party-state overlay	India, Phillippines, Malaysia, China
C	L1, T2-Nominal: Newly-legislated, in early operationalisation	Pakistan
D	L3: Policy/decree-led with weak enforcement	Indonesia, Bangladesh, Papua New Guinea, Myanmar
E	L4, T4: Fragmented or absent	Nepal, Afghanistan

Limitations

Non-English-language legal and policy debate is likely under-represented for China, Indonesia, Myanmar, South Korea and Bangladesh, particularly in domestic civil society and academic commentary.

The country's evidence base is also uneven. Coverage is rich for some countries (China, Indonesia, India, Philippines) and notably thinner for Afghanistan and Myanmar, where access restrictions and the contested legitimacy of the governing authorities limit independent reporting.

For Papua New Guinea and Pakistan, the legal architecture has been substantially reset within the research window. PNG launched SevisPNG on 24 November 2025 and Pakistan enacted the Digital Nation Act on 29 January 2025. The source base for these two countries therefore reflects an early operational period.

A small number of country data points, notably for Nepal, were drawn from independent journalism and practitioner commentary where government primary sources were thin. These were used cautiously, and the underlying footnoted primary sources were consulted in preference where available.

The DPI legal landscape is also evolving rapidly. Four developments material to these findings fell inside the research window. Pakistan's Digital Nation Pakistan Act was enacted on 29 January 2025. Papua New Guinea launched SevisPNG on 24 November 2025. India activated the DPDP Act and accompanying Rules on 13 November 2025. South Korea's National Assembly passed amendments to the Personal Information Protection Act in February 2026 (promulgated March 2026, effective September 2026). These findings should accordingly be read as a snapshot of early 2026.

The analysis assesses the *architecture* of oversight and legal foundations, namely what bodies exist and what laws are in force, rather than the *implementation quality* of either. Implementation-level questions, such as whether grievance redress is accessible to citizens, whether transparency mechanisms function and whether civil-liberties risks are materially mitigated, are not within scope here.

4. Who Shapes DPI in APAC? A Comparative Study of Consultation Practices in DPI Governance

By Jeremy Htet

Background

Existing studies do not fully state how participatory DPI governance should be. Some approaches emphasize expert-led design, especially for digital IDs and payment systems, where security, interoperability, and implementation capacity are central; technical criticality was embedded in early framework DPI implementations (Eaves & Rao, 2025). Conversely, other approaches argue that because DPI shapes access to services, data rights, and state-citizen relationships, it must be governed through more open, structured, and democratically aligned consultation (Seth et al., 2023). For this interim comparison, the key issue is not whether consultation exists at all, but whether it is structured, documented, and capable of incorporating stakeholders' inputs, especially the feedback of ordinary people into active DPI governance.

Definition and baseline in this study

For this study, a formal consultation mechanism is defined as a structured, official process through which governments systematically collect, document, and utilize multi-stakeholder feedback to guide Digital Public Infrastructure (DPI) design, implementation, and regulation. Drawing from the Universal DPI Safeguards Framework established by the United Nations Office for Digital and Emerging Technologies - UN ODET and UNDP, this concept emphasizes an institutional transition away from internal state decision-making or expert-level conversations. Instead, it prioritizes a recognized, transparent platform where a wide range of actors, including citizens, technical experts, local businesses, and civil society organizations, can actively integrate insights before or during pivotal DPI policy phases. Without formalized and documented civic consultation platforms, large-scale digital infrastructure triggers widespread exclusion, degrades public trust, and systematically violates the rights of data privacy of the citizens.

The baseline used here is **not full public participation**. Instead, the comparison asks whether a country has **a visible and institutionalized consultation process** (e.g MyGov in India) that goes beyond internal government coordination or informal stakeholder engagement. This matters because DPI systems affect identity, payments, data exchange, and access to public services, so a visible consultation mechanism is the way to improve legitimacy, promote public trust, and reduce the systemic exclusion by the government. Countries are therefore measured against a minimum standard of structured, policy-relevant consultation process, not against full public participation.

Findings

A first pattern is that the most formalized consultation mechanisms tend to appear in countries with stronger regulatory capacity and more institutionalized policy processes. India stands out because the Ministry of Electronics and Information Technology (India) MeitY and My Government (India Citizens Platform) - MyGov provide visible channels for consultation on draft policies and DPI-related initiatives (Maheshwari & Sharma, 2025). Australia uses the Regulatory Impact Statement - RIS process to require structured assessment and consultation on major regulations, including digital regulations (Goggin et al., 2019). Nepal also appears relatively strong in this dimension because its Digital Transformation Project includes a Stakeholder Engagement Plan and a Project Implementation Unit to manage consultation across the project cycle (Nepal Digital Transformation Project, 2025). The Papua New Guinea government officially endorsed the National Digital ID Policy 2025, which establishes core Digital Public Infrastructure (DPI) systems like the SevisPass digital ID and SevisWallet. To ensure public participation, the Department of Information and Communications Technology (DICT) uses its official portal (ict.gov.pg) as a formal platform for civic consultation. Through this digital channel, citizens and civil society can directly review policy drafts and submit feedback to shape the country's ongoing digital identity and sovereign AI strategies (Department of Information and Communications Technology, 2026).

A second pattern demonstrates that several countries rely on expert-driven or sectoral consultation rather than broad public participation, organizing their frameworks strictly around state agencies, technical actors, and market monopolists. For example, Singapore's GovTech manages Singpass updates through a business-to-business (B2B) ecosystem and closed pilot integrations with financial enterprises rather than open public consultation (World Bank, 2022). Similarly, Indonesia established its QRIS payment by restricting consultation to institutional working groups within the Indonesian Payment System Association (ASPI) and commercial fintech operators to prioritize rapid ecosystem interoperability (Bank Indonesia, 2019). Furthermore, South Korea channels its digital governance through specialized administrative mechanisms such as financial regulatory bodies under the Special Act on Financial Innovation Support, which purposefully confine data-sharing and regulatory debates to state ministers, scientific expert boards, and industrial startups (OECD, 2017). Consequently, while structured consultation exists across these countries, it remains strategically operated within specialized networks considered directly relevant to technical deployment and system engineering.

A third pattern is the prominence of project-by-project or centralized consultation in countries where DPI governance is narrower or less institutionalized. Malaysia, Pakistan, and Bangladesh show some consultation activity, but it is usually tied to specific projects, or milestones, government-business coordination, or selected stakeholder engagement rather than a system-wide public consultation framework (AfricLaw, 2026; Digital Rights Foundation, 2023; Economic Planning Unit, 2021). These cases suggest that consultation may be present as an ad-hoc administrative process without becoming a durable, legally mandated governance mechanism.

A fourth pattern is that Myanmar and Afghanistan appear at the weakest end of the spectrum. In both cases, extreme political conditions and heavily centralized rule leave little or no space for documented DPI-specific public consultation (Access Now, 2024; Freedom House, 2024; SEAP, 2025). These are not simply weaker variants of other developing frameworks. Rather, they reflect a more fundamental, structural absence of civic participation and digital rights oversight in national digital governance.

A clear pattern shows that most countries do not build their Digital Public Infrastructure (DPI) alone. Instead, they rely heavily on **international organizations and bilateral partnerships**. It was more significant in the case of Nepal's Digital Transformation Project, Myanmar's bilateral cooperation with India and PNG's National Digital ID Policy. While few countries like India design their own sovereign systems, developing economies like Nepal and Papua New Guinea depend on the funding and guidance of global lenders like the World Bank and the Asian Development Bank (ADB). Remarkably, even Singapore has some collaboration with the World Bank in implementing their Singpass platform. At the same time, two-country partnerships are also crucial. A prime example is India's Global Digital Public Infrastructure Repository (GDPIR), a G20-backed platform created specifically to share technical blueprints and help smaller nations design and launch secure, population-scale digital systems. Ultimately, completely independent national DPI development is rare, as most countries rely on **cross-border cooperation** and **loan or grant of development finance institutions such as the World Bank and ADB** to build their digital infrastructure.

5. Who Can Citizens Turn To? Accountability Through Grievance Redress and Transparency in Asia-Pacific Digital Public Infrastructure

By Khushbakht

Background and literature

The World Bank Group's 2025 approach document on DPI and development (World Bank, 2025a) establishes coordinated oversight and accountability as preconditions for sustainable DPI. The document argues that digital systems operating at population scale require institutional arrangements capable of responding to failures, not just delivering services. The United Nations Development Programme' (UNDP) 2023 framework paper (UNDP, 2023) makes a parallel argument by framing enabling governance as one of three foundational pillars of DPI, alongside open technology and competitive markets. Governance here includes not only the bodies that make decisions but the mechanisms through which those decisions can be questioned. As the World Bank puts it, DPI should avoid the risk of becoming obsolete by prioritising *outcomes and use cases*, which implies feedback loops between citizens and systems.

Mazzucato et al. (2024), go further, arguing that transparency and accountability are not simply operational features of DPI but core expressions of its public character. Their University College London (UCL) Institute for Innovation and Public Purpose paper introduces five pillars for what makes infrastructure genuinely public, two of which are directly relevant here: transparency and accountability as a distinct pillar, and co-creation and participation as another. Their argument is that DPI which lacks these properties may carry the label of public infrastructure while functioning more like a proprietary system. The citizen becomes a user rather than a stakeholder.

Seth et al. (2023), writing about India's experience, provide a more operational version of the same concern. Their governance framework proposal calls for public oversight across three distinct phases of DPI development: conceptualisation, technical design, and active platform management. The absence of grievance channels, they find, is not simply a regulatory gap but a design choice that concentrates risk in the people least able to absorb it. The paper identifies the wrongful exclusion of marginalised communities from welfare benefits and frequent transaction failures as consequences of systems built without accountability infrastructure.

Eaves and Rao (2025) offer a measurement framework that is analytically useful for this comparison. They define DPI across three dimensions: underlying technology, embedded public-interest values, and societal adoption context. Grievance redress and transparency both fall within the public-interest values dimension. Their framework suggests that systems scoring highly on technological deployment but poorly on public-interest values represent an incomplete

and potentially harmful form of DPI. This distinction between deployment and accountability is the central analytical thread in this study.

The European Union's General Data Protection Regulation (GDPR) (European Parliament and Council, 2016) serves as the de facto global benchmark for data protection accountability architecture. Its paired model of a comprehensive primary regulation alongside independent national data protection authorities provides the comparative baseline against which APAC arrangements are implicitly assessed throughout the literature. The GDPR matters here not as a prescription but as a reference point that shows what a fully developed accountability architecture looks like in practice.

Where the existing literature is weakest is on grievance redress specifically in the context of DPI infrastructure failures, as opposed to data protection complaints. Most studies address complaints as a subset of privacy law. The conflation is understandable but analytically costly. A payment failure, a wrongful exclusion from a biometric welfare programme, or an identity system error are infrastructure failures that may or may not have a data protection dimension. The practical consequence is that many countries have data protection complaint bodies but no DPI-specific channel, leaving citizens who experience infrastructure failures with no clear institutional home for their complaint. This gap recurs across almost every country in the dataset in this study.

This study draws a clear line between DPI infrastructure failures and data protection complaints. A country can have a working data protection authority and still leave a citizen with nowhere to go when their biometric read fails, their payment is blocked, or their identity record contains an error. These are infrastructure problems that may have nothing to do with data protection law. Treating them as the same thing overstates how much protection citizens actually have. This distinction is what the comparison is built on.

On transparency, the Organisation for Economic Co-operation and Development's (OECD) 2025 Digital Government Review of Korea notes that South Korea ranks first in the OECD Digital Government Index according to the most recent available ranking and operates proactive information disclosure under the Official Information Disclosure Act (OECD, 2025). However, the same review finds that most published data consists of administrative authorisation documents rather than substantive DPI policy content, which complicates any simple correlation between disclosure volume and governance quality. Even the most advanced transparency architecture in the dataset does not automatically produce citizen-facing accountability.

Competing views on how much transparency is feasible exist in the literature. Some approaches, particularly those emphasising security-by-design in identity systems, argue that full public disclosure of governance architecture creates vulnerabilities. The World Bank and GovTech Singapore's 2022 joint case study on Singapore Personal Access (Singpass) and API Exchange (APEX) (World Bank, GovTech, 2022) is an example of documentation that provides substantial technical transparency for a practitioner audience while not serving citizen-facing

accountability needs. This tension between expert transparency and citizen transparency is an underexplored dimension of the existing conversation.

Definition and baseline in this study

1. Grievance Redress Mechanism

For the purposes of this study, a grievance redress mechanism is defined as a formal channel through which citizens or affected individuals can raise complaints, seek remedy, or challenge decisions relating to DPI systems. This covers failures across all three core DPI layers: digital identity errors, payment disputes, and data exchange or sharing violations. It includes dedicated DPI complaints bodies, data protection commissions with DPI jurisdiction, judicial review rights, and ombudsman-type channels.

The definition draws on the World Bank Group's framing of accountability infrastructure as a precondition for viable DPI (World Bank, 2025a), and on the finding from an academic impact evaluation of Pakistan's Pakistan's Benazir Income Support Programme (BISP) biometric programme (World Bank, 2022) that grievance redress mechanisms are needed to address technology and process failures that prevent beneficiaries from accessing payments they are entitled to. This matters because the source is not a critique of DPI but an evaluation that found meaningful welfare benefits for women recipients. Even a study documenting those benefits identified the absence of grievance redress as a risk that could undermine them.

The comparison standard for this dimension has three tiers. Best practice refers to a statutory, independent, DPI-specific or DPI-applicable grievance channel that citizens can access without cost, with enforceable outcomes and a defined resolution timeline. Australia's Digital ID Act 2024 redress framework is the only example in this dataset that meets this standard. Partial refers to a general data protection complaints body that covers DPI-adjacent harms but is not DPI-specific and lacks a dedicated DPI mandate. Absent refers to conditions where no complaints body exists, no judicial review is available, or judicial review has been explicitly barred by law. The GDPR model, pairing a comprehensive statute with an independent national authority, is what the Best Practice tier approximates in the DPI context.

2. Transparency and Public Access to DPI Information

Transparency and public access to DPI information refers to the extent to which citizens can access information about how DPI systems are designed, governed, and operated. This includes published policy documents, governance frameworks, implementation progress reports, independent audits, and mechanisms through which citizens can trace how DPI decisions are made and by whom.

The definition draws on Mazzucato et al.’s (2024) argument that transparency is not a peripheral feature of public infrastructure but one of its defining properties. It also draws on Eaves and Rao's (2025) framework suggesting that systems scoring highly on deployment but poorly on

public-interest values, including transparency, represent incomplete DPI. The comparison standard has three tiers. Best practice refers to proactive publication of DPI strategy documents, implementation progress, and consultation feedback summaries through multiple public channels, with independent monitoring mechanisms. Partial refers to conditions where DPI information is published but fragmented across agencies, primarily expert-facing, or covers policy intent without implementation accountability. Absent refers to no accessible DPI governance documentation, or information that is confined to government and expert circles, or that is actively suppressed.

These two dimensions matter for a connected reason. Grievance redress asks whether a citizen who is harmed by a DPI system has anywhere to go. Transparency asks whether a citizen who wants to understand a DPI system can find out how it works. Together, they determine whether DPI is governed for the people it serves or primarily for the state and institutions that operate it. Where both are absent simultaneously, DPI ends up serving the institutions that operate it more than the people it is meant to serve. Pakistan illustrates this more sharply and is the primary focus of the findings. But the patterns extend across multiple countries in the dataset and reveal structural conditions affecting the region as a whole.

Findings

The fourteen countries fall into four broad positions on both dimensions. Reading them together reveals a regional pattern more consistent than a country-by-country account would suggest. The main finding from this comparison is that having a law does not automatically mean citizens are protected. What matters is whether the law creates real accountability mechanisms or removes them. Two things seem to drive which cluster a country falls into: how open the political system is, and whether civil society is organised enough to push back on governance design. Pakistan is the most important exception to the general pattern. It is a democracy with active civil society, yet it has enacted the only explicit removal of judicial review in the dataset. The clusters below make the regional pattern visible, but the exceptions reveal the most.

Country	Grievance Redress	Transparency and Public Access
Australia	Best practice – statutory DPI-specific framework	Best practice – proactive publication, multi-channel feedback
South Korea	Partial – formal channels, weak DPI-specific response	Partial – strong general transparency infrastructure
Singapore	Partial – Personal Data Protection Commission (PDPC) jurisdiction, no DPI-specific body	Partial – technical documentation public, governance opaque

India	Partial – Unique Identification Authority of India (UIDAI) self-administered, no cross-DPI body	Partial – international-facing, not citizen-facing
Philippines	Partial – National Privacy Commission (NPC) jurisdiction, no DPI-specific channel	Partial – electronic Freedom of Information (eFOI) limited to executive branch
Malaysia	Absent – fragmented agency channels, no unified body	Partial – strategy documents public, no independent monitoring
Indonesia	Absent – no data protection authority established	Partial – Satu Data initiative, trust deficits persist
Nepal	Absent – general channel only, no DPI mandate	Partial – deteriorating, opaque social media ban
Bangladesh	Absent – no grievance mechanism documented	Absent – no consolidated DPI information system
Papua New Guinea	Absent – aspirational policy language, no legal force	Minimal – one draft document publicly accessible
Pakistan	Absent – judicial redress legally barred by statute	Absent – fragmented, accountability actively removed
China	Absent – state-controlled private platforms only	Absent – no public transparency, state-directed
Myanmar	Absent – DPI weaponised against citizens	Suppressed – transparency actively suppressed
Afghanistan	Absent – DPI used as instrument of repression	Suppressed – transparency suppressed since 2021

Reading across both dimensions, the fourteen countries fall into four clusters. These clusters make the regional pattern more visible than a country-by-country account.

Cluster	Description	Countries
Best Practice	Statutory, DPI-specific grievance and transparency frameworks with enforceable outcomes and proactive publication.	Australia
Partial Accountability	Data-protection bodies or complaint channels exist, but none are DPI-specific; transparency is fragmented or expert-facing.	Singapore, India, South Korea, Philippines

Aspirational Frameworks	Policy frameworks documented but grievance mechanisms unestablished; transparency incomplete or deteriorating.	Malaysia, Indonesia, Nepal, Bangladesh, Papua New Guinea
Absent Accountability	No grievance or transparency architecture; accountability either deliberately removed by statute or structurally impossible under authoritarian governance.	Pakistan, China, Myanmar, Afghanistan

The One Country That Meets the Standard: Australia

Australia stands apart from every other country in this dataset on grievance redress. The Digital ID Act 2024 is the only statute in the set that creates a DPI-specific redress framework with enforceable outcomes. Phase 1, the Digital ID Amendment (Redress Framework and Other Measures) Rules 2025, commenced 19 November 2025. It requires accredited providers to notify affected individuals, publish complaint-handling policies, and escalate unresolved complaints within 28 days. Phase 2, currently in public consultation in early 2026, proposes statutory rights to a formal apology, a structured explanation, and financial compensation for harm caused by fraud or technical lockout. Australia's regulatory framework requires that all significant digital regulations undergo a publicly available cost-benefit assessment through the Regulation Impact Statement process administered by the Department of the Prime Minister and Cabinet. This combination of a DPI-specific statute, a published implementation framework, and consultation with published feedback summaries represents the best practice benchmark for this comparison.

Australia presents a mature and procedurally regulated framework that extends beyond the Digital ID Act itself. The Digital ID Act is not the whole story: it operates alongside a Co-regulation framework between the Australian Competition and Consumer Commission and the Office of the Australian Information Commissioner, and the redress rules are themselves a product of a multi-stage public consultation process. This procedural depth is what distinguishes Australia from countries that have comparable aspirations but incomplete architecture.

Partial Accountability: Singapore, India, South Korea, and the Philippines

Singapore, India, South Korea, and the Philippines each have data protection bodies with jurisdiction that extends in principle to DPI-adjacent harms but none has a DPI-specific grievance channel. Singapore's Personal Data Protection Commission (PDPC), established under the Personal Data Protection Act 2012 (Government of Singapore, 2012), handles personal data misuse complaints including those involving Singpass and PayNow. However, individuals cannot sue organisations directly and technical DPI failures are referred back to individual service providers. This means that a citizen harmed by a DPI failure may find themselves passed between agencies with no clear point of accountability, which falls short of the best practice standard defined in Section 2.1 (Association of Banks in Singapore, n.d.; GovTech Developers Portal, n.d.). Singapore's Public Sector (Governance) Act 2018

(Government of Singapore, 2018) governs data sharing across government agencies and closes the gap that the PDPA leaves for public sector actors, which is a more complete statutory design than most countries in this set.

India's Unique Identification Authority of India (UIDAI) operates a multi-channel complaints system for Aadhaar, including a toll-free number and an online portal. However, this is self-administered by the DPI operator itself with no external adjudicator. Citizens harmed by failures beyond Aadhaar, such as Unified Payments Interface (UPI) disputes or data sharing without consent, have no equivalent unified channel (NASSCOM, 2024). The activation of India's Digital Personal Data Protection Rules on 13 November 2025 established a statutory Data Protection Board, which provides an independent redress route for data protection complaints, including those involving DPI systems. This does not amount to a DPI-specific grievance channel, but it narrows the gap that existed before. On transparency, India's Global Digital Public Infrastructure Repository is a global policymaker resource, not a domestic citizen-facing transparency mechanism (Government of India, n.d.). DPI governance information for ordinary citizens remains fragmented across the Ministry of Electronics and Information Technology (MeitY), National Institution for Transforming India (NITI) Aayog, and the Reserve Bank of India.

South Korea is the second-strongest on transparency in the dataset, operating proactive information disclosure under the Official Information Disclosure Act and ranking first in the Organisation for Economic Co-operation and Development (OECD) Digital Government Index according to the most recent available ranking (OECD, 2025) The Digital Platform Government initiative, launched in 2022, includes a system allowing citizens to check who accessed their data. However, South Korea's DPI-specific accountability record is the most surprising negative finding in this comparison. A November 2023 outage of the Government24 and Saeol portals lasted 56 hours and generated 240,000 complaints. The available sources do not document what formal redress, if any, affected citizens received, nor whether the outage prompted institutional reforms to DPI-specific complaint handling. This gap between a sophisticated formal transparency architecture and the absence of documented DPI-specific accountability is what places South Korea in the Partial cluster rather than closer to the best practice standard.

The Philippines has the National Privacy Commission (NPC), established under the Data Privacy Act of 2012, with jurisdiction over both public and private sector entities. This makes the Philippines unusual in the dataset: most data protection authorities exclude the public sector. The electronic Freedom of Information (eFOI) portal operates under an executive order. However, a Freedom of Information bill has been filed in every Congress since the eighth without passing, meaning transparency remains executive policy rather than statutory right (Kapur & LaForge, 2026).

Aspirational Frameworks Without Functioning Mechanisms: Malaysia, Indonesia, Nepal, Bangladesh, and Papua New Guinea

Malaysia, Indonesia, Nepal, Bangladesh, and Papua New Guinea all have documented DPI policy frameworks but no operational grievance mechanism and incomplete transparency architecture. In each case the gap reflects institutional non-establishment rather than deliberate removal. Malaysia's planned National Data Commission under the 13th Malaysia Plan (RMK-13) could eventually fill the gap but remains at the planning stage as of 2025 (Gobind Singh Deo, 2025). Indonesia's Personal Data Protection Authority was mandated by the 2022 Personal Data Protection (PDP) Law but remained unestablished as of early 2026. A June 2024 ransomware attack on Indonesia's Temporary National Data Centre exposed millions of citizens' data with no formal redress channel in place. Bachtiar (2025) identifies trust deficits and decentralised governance as persistent structural obstacles in Indonesia. Bangladesh's Global Development Network (GDN) working paper recommends improving data governance laws and building unified portals, confirming that both are absent (Raihan et al., 2025). Papua New Guinea's draft National Digital ID Policy 7.2 describes a user-centric model in aspirational terms but, as a draft with no legal force, creates no citizen-facing complaint channel (Department of Information and Communications Technology Papua New Guinea, n.d.).

Pakistan: The Sharpest Case in the Dataset

Pakistan does not belong to the third cluster. It occupies a distinct category because the absence of grievance redress is not a product of institutional incompleteness but of deliberate statutory design. The Digital Nation Pakistan (DNP) Act, 2025 simultaneously creates the most explicit DPI governance structure in the dataset and removes the principal mechanism through which citizens could challenge that structure.

- The formal architecture created by the Act. The Digital Nation Pakistan Act, 2025 establishes three bodies: the National Digital Commission (NDC) chaired by the Prime Minister and including four provincial Chief Ministers, the State Bank of Pakistan (SBP), the Federal Board of Revenue (FBR), the Pakistan Telecommunication Authority (PTA), and the Pakistan Digital Authority (PDA); the Pakistan Digital Authority as the central implementing body constituted in August 2025; and an Oversight Committee established as an independent review body reporting to the NDC. Pakistan also has mature foundational layers in National Database and Registration Authority (NADRA), which has operated as the central biometric identity authority since 2000, and Raast, the State Bank of Pakistan's instant payment system (Government of Pakistan, 2025).

- What Section 29 of the same Act does. Section 29 provides, in terms, that no decision or action taken under the Act shall be questioned by any agency or challenged in any court or tribunal, nor shall any injunction be granted against such decisions or actions (Government of Pakistan, 2025). This is not a policy gap. It is a written, enacted, and judicially operative clause. The Pakistan Digital Authority is the

body that implements and operates the National Data Exchange Layer (NDXL), which is designed to connect major government databases including those held by NADRA, the Federal Board of Revenue, and health ministries. Section 29 means that a body with access to the most sensitive personal data in the country cannot be taken to court by the people whose data it manages. Judicial review is not simply unavailable. It is statutorily barred. The Oversight Committee within the Act reports to the NDC, which is chaired by the Prime Minister. It is not independent of the executive branch.

- The missing data protection law. Pakistan's Personal Data Protection Bill (PDPB) was drafted in 2023, approved by Cabinet, and has not been passed by Parliament (Ministry of Information Technology and Telecommunication, 2023). The International Comparative Legal Guides (ICLG) Data Protection Laws and Regulations Report 2025 to 2026 on Pakistan confirms that the proposed National Commission for Personal Data Protection is not in existence (International Comparative Legal Guides, 2025). This resolves the potential conflict with a Wikipedia entry describing the Commission as active since 2023. Even in draft form, the bill's independence was already in question: Digital Rights Foundation's (DRF) analysis found the proposed Commission would remain under Federal Government administrative control, undermining the independence the body was meant to provide (Digital Rights Foundation, 2023). The bill's own Statement of Objectives specified that it would come into force not beyond two years from the date of promulgation. The transition period never started because the law was never promulgated.

- The governance frameworks that do not yet exist. The World Bank's January 2025 implementation progress report on the Digital Economy Enhancement Project (DEEP) (World Bank, 2025b) shows that the indicators for the Pakistan Digital Government Data Governance and Interoperability Framework adopted and the Pakistan Digital Government Institutional Framework adopted both record a baseline of No, a current value of No, and a target of Yes by November 2027. The NDXL is being built while the frameworks that would govern who can access what data under what conditions remain future targets. The World Bank's own 2023 Project Information Document (World Bank, 2023) acknowledged that the data protection bill had been drafted but that further work was needed and that the domestic data economy should not be unduly restricted. The $78 million DEEP project was approved despite this admission. As of December 2024, the World Bank progress report records zero transactions on the National Data Exchange Layer, zero entities integrated to the NDXL, and zero services available on the national citizen services portal. The technical build-out, often described as moving faster than the legal framework, is itself behind schedule (World Bank, 2025b).

- In 2024, a Joint Investigation Team confirmed that details of 2.7 million citizens were illicitly taken from NADRA between 2019 and 2023 by employees at offices in Karachi, Multan, and Peshawar (Ahmed, 2025). Criminal proceedings were launched

but affected citizens had no dedicated data protection authority or DPI-specific grievance body to turn to at the time, since no such law or body existed until 2025. The governance gap has not since closed, only shifted: the Pakistan Digital Authority (PDA), which now operates the National Data Exchange Layer connecting to NADRA's data holdings, is itself shielded from court challenge under Section 29 of the DNP Act, enacted a year after the breach was confirmed. A citizen harmed by a comparable failure today would face the same absence of recourse, now backed by statute rather than simple absence of one.

- The BISP finding and why it makes the governance gap sharper, not softer. A multi-institutional academic evaluation (World Bank, 2022) studied what happened when Pakistan's BISP programme switched to biometric verification for cash payments to women. The headline finding is positive: biometric verification more than tripled the probability that women collected their own cash directly, an increase of 46 percentage points. Before this system, many women had to send male relatives to collect on their behalf. The same evaluation found that satisfaction dropped from 72 to 54 percent, that the process initially more than doubled the difficulty of withdrawing cash, and that grievance redress mechanisms are needed to prevent exclusion due to technology or process failures. This source matters analytically because it is the strongest available evidence of a genuine DPI inclusion benefit in Pakistan, and even that source identified the absence of grievance redress as a risk. The government built a system that its own evaluators said needed accountability structures, and then passed a law removing the main accountability mechanism that would have been available.

- On transparency specifically. Pakistan's DPI plans are split across multiple agencies with almost no public documentation of how they connect. The Data Governance and Interoperability Framework that would define who can access what data does not yet exist to be published. Section 29 eliminates judicial review, which is one of the mechanisms through which disclosure can be compelled in law. The Friday Times investigation reports that citizens cannot identify who is responsible for DPI decisions (Ahmed, 2025). The result is not a transparency deficit in the sense of inadequate communication. It is a structural condition in which the information that would make accountability possible has no institutional home.

Suppressed Accountability: China, Myanmar, and Afghanistan

China, Myanmar, and Afghanistan represent a qualitatively different category. The absence of grievance redress and transparency in these countries is not a governance gap to be addressed. It is a governance design. What China, Myanmar, and Afghanistan share is that there is no separation between the state and any body that could check it. In China, the same party-state system that runs DPI also controls the complaint channels, so accountability never reaches an independent body. In Myanmar, DPI has been turned into a surveillance tool rather than a public service. In Afghanistan, the institutional conditions for independent oversight do

not exist at all. This is different from the aspirational cluster, where the gap could in principle be filled by reform. In these three cases, the political conditions that make independent accountability possible are absent and actively prevented.

In the payments domain, citizen complaints in China are routed primarily through state-authorised private platforms including Alipay and WeChat Pay, with no independent adjudicator (Zeng & Kim, 2025). Academic analysis finds the legislative framework for consumer protection in mobile payment services insufficient. Complaints touching on political or governance matters are censored (Nieborg, n.d.; Yang, 2023). The state-controlled complaint channels operate with no published governance framework accessible to citizens.
Myanmar under the State Administration Council presents the clearest case of DPI used as a tool of surveillance rather than service. The 2025 Cybersecurity Law criminalises Virtual Private Network (VPN) use and mandates platforms to provide unrestricted government data access. The junta's Person Scrutinization and Monitoring System combines facial recognition, artificial intelligence, and electronic identity documents. Human Rights Myanmar's 2025 UN submission describes Myanmar as a digital dictatorship. Myanmar Internet Project documented 105 internet shutdown instances in 2025 alone.

Afghanistan under the De Facto Authorities presents a parallel case. Flensburg, Lai, and Lehmann-Jacobsen (2025) confirm that the Taliban controls internet infrastructure and uses it for censorship and surveillance. Approximately 40 percent of Afghans do not hold the Tazkira identity document, meaning a significant portion of the population is excluded from basic service access (SEAP, 2025). The pre-2021 e-Tazkira rollouts were themselves politically contested due to the mandatory national label controversy that sparked protests from ethnic minorities (Library of Congress, 2018). Shires and Wilkinson (2024) document how both technical and sociopolitical resilience of internet infrastructure have been systematically eroded since the Taliban takeover.

Cases against the pattern

South Korea's DPI-specific incident response is the most unexpected finding in this dimension. South Korea has the most developed general transparency infrastructure in the dataset. Its formal complaint mechanisms are among the most sophisticated. Yet the November 2023 Government24 outage and the government's response reveal a gap between formal mechanisms and functional DPI accountability that is more characteristic of a Cluster Three country. This suggests that general digital government maturity does not automatically translate into DPI-specific accountability.

Pakistan is surprising in the opposite direction. Among developing countries with ambitious DPI programmes, it is unusual in having a dedicated DPI statute. The expectation would be that a dedicated statute produces stronger accountability. Pakistan demonstrates the opposite: the statute creates the formal architecture while simultaneously removing the accountability mechanism that would make that architecture meaningful.

A third surprising finding goes in a different direction. The Philippines sits in the Partial cluster, alongside Singapore and India. But on one specific point its accountability architecture is actually stronger than either. The National Privacy Commission covers both public and private sector entities. Singapore's data protection authority excludes public agencies. India's UIDAI complaints system is run by the same body that operates Aadhaar, meaning the operator and the adjudicator are the same institution. The Philippines does not meet best practice overall, but this comparison shows that Partial does not mean uniformly weaker than the countries ranked above it.

The single most important takeaway from this comparison is that grievance redress and transparency are the dimensions where the gap between DPI form and DPI function is most visible. The correlation between statutory ambition and accountability outcome is weak across the dataset. What predicts accountability is not the existence of a law but whether that law creates, rather than removes, the mechanisms through which citizens can seek remedy and understand how systems that govern their lives actually operate.

Limitations

The most significant limitation is that this study assesses the architecture of grievance redress and transparency, which bodies exist and what frameworks are in place, rather than the quality of those mechanisms in live practice. Whether a published DPI strategy document is actually accessible to citizens without internet access or digital literacy, whether a complaints channel is genuinely reachable for rural or low-income populations, or whether a statutory right translates into meaningful resolution, cannot be answered from public secondary sources.

Urdu-language public debate about data protection and grievance redress is not represented. This is a significant gap because the communities most affected by DPI failures are least likely to participate in English-language policy debates. Known sources that would be relevant if accessible include Urdu-language publications by the Digital Rights Foundation, reporting in Geo News and Dawn's Urdu edition on the NADRA breach proceedings, and Pakistani legal scholarship published through university law journals. Closing this gap would require a researcher with Urdu-language proficiency working within the Pakistani policy context.

6. Serving or Surveilling? Surveillance Risk and Civil Society Oversight in Asia-Pacific DPI

By Fatima Rezaie

Background and literature

Digital Public Infrastructure (DPI) has emerged as a primary mechanism through which governments deliver services, manage identity, and facilitate financial transactions at scale. As digital systems become more deeply embedded in public life, with an estimated 6.12 billion smartphone users globally as of 2026 that represent approximately 74% of the world's population (Datareportal, 2026), questions of how governments monitor and regulate activity on these platforms have become central to DPI governance scholarship. Surveillance, broadly understood as the observation and collection of data on individuals by institutions, sits at the intersection of security, accountability, and rights.

Defining Surveillance from multiple angles

The concept of surveillance does not have a single settled definition. Different scholarly and legal traditions emphasise different aspects of the phenomenon, and these differences have practical consequences for how surveillance is evaluated and governed.

From a historical and critical theory standpoint, surveillance carries a predominantly negative connotation. From the mid-twentieth century onward surveillance has been construed as a fundamental threat to freedom and liberty, not only in authoritarian states but also in democracies (Hintz et al., 2022). This negative valence, rooted in the idea of the watched being controlled by the watcher, became the foundation of much social and legal criticism of government monitoring practices.

In the strictly legal domain, particularly in US law, surveillance refers to "the act of observing another in order to gather evidence," which may be covert or overt (Legal Information Institute, 2021). This framing is narrower and procedural: it concerns the means and authorisation of observation, not its broader social effects.

A broader technology-focused definition is offered by the Freedom Online Coalition, which describes surveillance technologies as products or services that can detect, monitor, intercept, collect, exploit, preserve, process, analyse, and retain sensitive data, personally identifying information (including biometrics), or communications concerning individuals or groups (Freedom Online Coalition, 2023). This definition is notable for acknowledging that such technologies can be used both lawfully with appropriate safeguards and in ways that are fundamentally unacceptable.

For the purposes of DPI governance research, the most analytically useful definition comes from sociologist David Lyon, as interpreted by legal scholar Neil Richards: surveillance is "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Richards, 2013, p. 1934, citing Lyon). This definition is broad enough to encompass both security-motivated monitoring and the routine administrative surveillance embedded in digital identity and payment systems, making it appropriate for studying DPI.

Why Surveillance Matters for DPI Governance

Scholars and civil society organisations have identified several interconnected reasons why surveillance is a critical governance dimension for DPI.

First, surveillance can chill the exercise of civil liberties. When people know or believe they are being observed, particularly those who voice their political opinions, they may self-censor and avoid controversial ideas. Richards calls this the threat to "intellectual privacy": the condition necessary for free minds to develop independently of state oversight (Richards, 2013). In the context of DPI, where identity, payment, and data systems are integrated and government-accessible, the chilling effect is amplified because the act of using essential services becomes the act of generating a surveillance record.

Second, surveillance creates power asymmetries between the watcher and the watched. The collection of personal information gives watchers power that can be exercised through blackmail, discrimination, and persuasion. Richards documents this across political systems: the FBI's surveillance of Martin Luther King Jr. to gather blackmail material; the use of surveillance files by former communist states in Eastern Europe to threaten political candidates decades later; and the Gadhafi government's use of telecommunications interception to identify and coerce dissidents (Richards, 2013). DPI systems, by centralising identity and transaction data, create infrastructure that can serve these purposes if governance safeguards are absent or eroded.

Third, surveillance enables sorting and discrimination. Consumer and government databases can profile individuals, assign them to categories, and allocate opportunities or enforce restrictions on that basis, what sociologist Oscar Gandy (1993) termed the “panoptic sort” (Richards, 2013). In DPI contexts this risk is acute: a digital identity system linked to social services, policing, and financial access can become the basis for systematic discrimination against marginalized groups if governance lacks independent oversight and redress mechanisms.

International organisations have also weighed in. The Freedom Online Coalition's Guiding Principles identify three areas of concern: the use of internet controls to suppress human rights and limit access to information; the pairing of video surveillance with AI-driven tools to identify and monitor people without legal basis; and the use of big data analytics to target individuals in

marginalised situations, including journalists, human rights defenders, and dissidents (Freedom Online Coalition, 2023).

Contested Territory and Gaps in the Literature

The literature does not present a unified view on where the line between legitimate and illegitimate surveillance should be drawn, especially in the DPI context. There is broad consensus that surveillance for national security purposes requires stronger justification and more robust oversight than for service delivery. However, the practical boundary is contested: DPI systems designed for service delivery routinely generate data that can be repurposed for security surveillance which is known as function creep.

Existing literature is also heavily weighted toward Western liberal democratic contexts. Research on US and UK legal frameworks, European data protection regimes, and civil liberties debates in anglophone democracies is abundant. Research on surveillance within DPI systems across South Asia and Southeast Asia, particularly in countries with weak civil society, limited judicial independence, or active conflict, is substantially thinner. This gap is directly relevant to the APAC countries in this study.

Definition and baseline in this study

Surveillance, in the context of DPI, means the capacity of a government or other actor to systematically collect, store, and act on personal data generated by people's use of these systems. This includes tracking who accessed which government service and when; linking identity data to payment records, health records, or social media activity; monitoring communications of individuals flagged as security risks; and profiling populations to allocate resources or enforce restrictions based on inferred characteristics.

DPI is not inherently a surveillance tool. The same infrastructure that delivers a benefit payment also generates a data trail. Whether that trail is protected, deleted, or used for secondary purposes depends entirely on governance: what laws govern data retention, what oversight bodies exist, whether individuals can access and challenge their own records, and whether systems are designed to minimise data collection in the first place.
For the purposes of this study, surveillance is defined following Lyon (as cited in Richards, 2013) as: the focused, systematic, and routine attention to personal details for purposes of influence, management, protection, or direction.

Applied to DPI governance, this study evaluates surveillance across three sub-dimensions:

- **Legal framework:** Does the country have laws that define, limit, and authorise surveillance? Are there independent oversight bodies? Is there a right to legal remedy for individuals whose data has been misused?

- **Technical architecture:** Are DPI systems designed with privacy-protective features, data minimisation, purpose limitation, decentralisation, or do they create centralised data stores susceptible to misuse?
- **Practice and risk:** What evidence exists of actual surveillance harms, chilling effects, discrimination, blackmail, or political targeting, enabled by or through DPI systems?

The baseline for evaluation draws on two sources. The first is the Freedom Online Coalition's Guiding Principles on Government Use of Surveillance Technologies, which represent an international consensus position on minimum conditions for lawful, rights-respecting surveillance. The second is the concept of intellectual privacy as articulated by Richards (2013): DPI governance should actively protect individuals' freedom to think, communicate, and organise without state monitoring as a default condition of using public digital infrastructure.

Findings

The following section presents findings across all ten countries. A summary comparative table is included below, followed by individual country assessments and cross-cutting pattern analysis.

Afghanistan

Afghanistan under the De Facto Authorities (DFA/Taliban) presents the most severe case of state-controlled digital infrastructure being used as an instrument of repression in this study. Prior to the Taliban takeover in 2021, digital infrastructure was already fragile and contested: the DFA had a history of targeting telecommunications towers, forcing mobile companies to shut or limit coverage (IMS, 2025).

During and after the 2021 takeover, the DFA used internet kill switches, located in backbone infrastructure managed through the Ministry of Communications and Information Technology (MCIT), to shut down internet access nationally and in specific regions as a means of suppressing protests and blocking media reporting. The DFA has blocked approximately 23 million websites including international media, civil society organisations, and independent local media. App bans, including TikTok and PUBG, have been implemented, with threats of broader bans on platforms including Facebook (IMS, 2025).

The DFA's relationship with social media is strategic and selective: platforms are allowed to continue because the DFA depends on them to distribute its own content and exercise influence, while technical controls and the threat of bans are used to pressure platforms on content moderation. This represents a sophisticated use of infrastructure control to leverage international commercial platforms while retaining coercive power over them. No meaningful DPI governance exists in terms of rights protection. Digital infrastructure is a tool of the state, and the state operates without accountability to those it governs.

Australia

Australia represents the clearest case among the ten countries of civil society concerns driving genuine policy change in DPI design. Early iterations of Australia's digital identity system were criticised for proposing a centralised model that would have created conditions for function creep (Salsa Digital, 2026; Factually.co, 2025). This critique was substantive enough to produce a structural redesign.

The Digital ID Act 2024 establishes the Australian Government Digital ID System (AGDIS) as an accredited, voluntary framework with explicit safeguards which include:

1. prohibitions on the use of single identifiers enabling comprehensive cross-agency profiling;
2. a prohibition on disclosing information for marketing; and
3. restrictions on the collection, use, and disclosure of biometrics (Australian Government, 2024).

The system is co-regulated by the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC). A redress framework exposure draft was put out for public consultation in early 2026, with private sector participation eligible from November 2026 (CPA Australia, 2025; Salsa Digital, 2026).

Australia's DPI approach involves voluntary participation, distributed architecture, independent co-regulation, statutory privacy protections which represents the strongest governance model among the ten countries assessed. Significant gaps remain: the system is nascent and the efficacy of the redress framework has not been tested.

Bangladesh

Bangladesh has an extensive biometric voter registration system and a growing digital government footprint, including the National Identity (NID) database which has become foundational for accessing a wide range of services. Bangladesh's DPI development has accelerated in recent years with digital service delivery platforms and mobile financial services reaching significant scale.

Surveillance risk in Bangladesh is moderate-to-high. The Digital Security Act 2018 is a broadly worded law that has been used to prosecute journalists, activists, and ordinary citizens for online speech (OHCHR, 2023). This has created a legal environment hostile to digital rights before it was replaced by the Cyber Security Act 2023. Critics, including Amnesty International and Human Rights Watch, have noted that the Cyber Security Act retains many of the same provisions that enabled misuse. The NID database and associated biometric infrastructure have been subject to significant data breach concerns, with a 2023 incident exposing personal data of millions of citizens (Amnesty International, 2024).

Bangladesh has limited independent data protection legislation and no dedicated data protection authority. Civil society space for scrutinising DPI governance is constrained by the legal environment, though human rights organisations continue to document abuses (Amnesty International, 2024)

India

India has one of the world's most extensive DPI ecosystems, built around three core layers: Aadhaar (biometric digital identity with over 1.3 billion enrolments), the Unified Payments Interface (UPI, processing billions of transactions monthly), and the Data Empowerment and Protection Architecture (DEPA) for data exchange. India's DPI is also being actively promoted internationally as a model for other nations, raising questions about what institutional assumptions travel with it (Tech Policy Press, 2024; CSIS, 2024).

The surveillance risk associated with India's DPI is high and primarily structural. The inclusion of biometrics (fingerprints and iris scans) in the foundational identity layer creates a surveillance-ready infrastructure even when the stated purpose is service delivery. For much of Aadhaar's operational life, no comprehensive data protection law governed this biometric data; the Digital Personal Data Protection Act was passed in 2023 but implementation rules remained incomplete as of 2026. The Supreme Court's 2018 Puttaswamy judgment established a constitutional right to privacy but enforcement against the DPI architecture has been partial (Rethink Aadhaar, 2025).

Civil society in India is active in scrutinising DPI governance, and the Ministry of Electronics and Information Technology's stated commitments to privacy-by-design are genuine. However, the gap between policy aspiration and implementation is wide, and documented cases of exclusion of vulnerable populations, particularly in welfare delivery, illustrate how DPI can harm the very people it is designed to serve (India Stack / exclusion documentation, 2026; NPR, 2018).

Indonesia

Indonesia launched INA Digital in 2024, comprising three core services: INA Ku (public service portal covering healthcare, education, and social aid), INA Gov (government administration portal), and INA Pas (digital identity system using facial recognition and liveness detection as a single sign-on gateway). A World Bank-backed project, supported by a US$250 million loan, underpins development of identity verification, e-KYC, digital ID, and data exchange infrastructure (Biometric Update, 2025; World Bank, 2026).

The surveillance risk associated with Indonesia's DPI is moderate-to-high and primarily structural. The inclusion of facial recognition in the INA Pas identity layer is significant: biometric data collected at scale creates a surveillance-ready infrastructure despite the stated purpose being service delivery. Indonesia's data protection legislation (the Personal Data Protection Law, passed in 2022) is relatively new and its enforcement mechanisms are not yet tested (Swiss German University, 2025; ICLG, 2025). Civil society capacity to scrutinise implementation is

limited, and the World Bank's involvement introduces some accountability around project standards without substituting for domestic governance.

Malaysia

Malaysia's government has been moving toward making MyDigital ID mandatory and has partnered MyDigital ID with the Royal Malaysia Police for prepaid SIM card verification, ostensibly to clamp down on cybercrime (Biometric Update, 2025; Malaysia4U, 2026). This police integration raises civil liberties concerns that are not fully documented in publicly available assessments. This action links a national digital identity system to police access without clear legal constraints on how that access is exercised, and is a significant structural risk.

These governance concerns are compounded by a federal audit of MIMOS, the agency building MyDigital ID infrastructure, which found RM28 million in unauthorised spending and shortfalls in security and project-management practices (The Edge Malaysia, 2026; Biometric Update, 2026). Financial governance failures at the infrastructure level amplify surveillance risk. A system built without rigorous security practices is both more vulnerable to external breach and more susceptible to internal misuse. Malaysia presents a case where several risk factors are accumulating simultaneously: movement toward mandatory participation, law enforcement integration, weak institutional oversight, and infrastructure security gaps.

Myanmar

Myanmar's DPI situation is shaped entirely by the military junta (State Administration Council, SAC) that seized power in February 2021 (Freedom House, 2024; Tech Policy Press, 2025). Institutional structures for data protection, civil liberties oversight, or judicial review of surveillance do not meaningfully exist under the SAC. The government department responsible for digital governance operates under junta authority.

The SAC has used telecommunications infrastructure and internet controls as tools of political repression, including targeted shutdowns, network restrictions, and surveillance of communications to monitor and suppress opposition activity (Access Now, 2025; Article 19, 2023). Prior to 2021, there was documented misuse of digital surveillance tools by the then-civilian government as well (Human Rights Myanmar, 2025). DPI development is effectively suspended or proceeding under conditions of total executive control without accountability. Myanmar represents a case, alongside Afghanistan, where the baseline conditions for rights-respecting DPI governance are entirely absent.

Nepal

Nepal is at an early stage of DPI development, with platforms including the Nagarik App, e-payment services, and digital land record systems (Digital Rights Nepal, 2025). DPI is highly centralised: a 2025 'Cyber Collapse' demonstrated the fragility of this architecture when a single

vulnerability in the Government Integrated Data Center (GIDC) halted digital services nationwide. The Information Technology and Cyber Security Bill remains in draft form, leaving gaps in the legal authority to penalise data breaches.

Surveillance risk in Nepal is driven by legislation and surveillance infrastructure deployment rather than by DPI governance per se. An Associated Press investigation and draft legislation revealed advanced surveillance technology deployment across public spaces alongside proposed digital laws that would significantly expand state control over communications (Nepal Explained, 2025). The Social Media Bill (2081) proposed heavy fines, imprisonment, and broad criminal liability for both platforms and users based on vaguely defined offences including harm to 'national interests' and pseudonymous use (Digital Rights Nepal, 2025). The bill was widely criticised by civil society, media, and digital rights experts for enabling censorship and chilling free expression (Digital Rights Nepal, 2025). In 2025, the government also intensified enforcement of social media directives and temporarily shut down unregistered platforms nationwide (S.S. Rana & Co, 2025; MediaNama, 2025).

Pakistan

Pakistan's DPI landscape is shaped by NADRA (National Database and Registration Authority), one of the region's oldest and most extensive biometric identity systems, and more recently by expanding digital government services and mobile financial infrastructure (Tribune Pakistan, 2025). Pakistan has a large and technically capable DPI base, though governance of that infrastructure has been persistently problematic from a rights standpoint.

Surveillance risk in Pakistan is high. The Prevention of Electronic Crimes Act 2016 (PECA) has been used extensively to prosecute journalists, opposition politicians, and ordinary citizens for online speech (RSF, 2025; Amnesty International, 2025). Amendments in 2022 and subsequent years expanded its scope. There are credible reports of ISPs being directed to deep-packet inspect traffic. NADRA's biometric database, while primarily a service delivery tool, has been accessed for law enforcement purposes without robust legal constraint (Springer / IJPCS, 2024; CIVICUS Monitor, 2025). Pakistan has no comprehensive data protection law as of 2026.

Philippines

The Philippines has an active DPI development agenda, anchored by the Philippine Identification System (PhilSys), a national digital identity system, alongside digital payment infrastructure and digital government service delivery platforms (World Bank, 2026). The Department of Information and Communications Technology (DICT) is advancing Digital Government Standards covering cybersecurity, digital ID, digital payments, and cloud governance.

Surveillance risk in the Philippines is moderate but with significant concerns. The National Privacy Commission (NPC) exists as a dedicated data protection authority, providing a degree of institutional oversight absent in many comparable countries (Digital Freedom Network

Philippines, 2026). However, the Philippines' political history, particularly the drug war under the Duterte administration and its use of surveillance and profiling of perceived opponents, demonstrates how state infrastructure can be weaponised when political will to protect rights weakens (Article 19, 2022). Civil society in the Philippines is active and vocal on digital rights issues, which is a meaningful constraint. The SIM Registration Act 2022, which requires national ID-linked SIM registration, has been criticised for enabling surveillance and exposing data without adequate protection (Article 19, 2022; Biometric Update, 2026). The PhilSys Act includes data protection provisions, but implementation remains partial.

Table 1: Comparative Overview of Surveillance Risk in APAC DPI Systems

Country	DPI Maturity	Surveillance Risk	Legal Safeguards	Civil Society Space
Afghanistan	Fragmented	Extreme	None	None
Australia	High	Moderate	Strong	Active
Bangladesh	Emerging	Moderate–High	Weak	Limited
India	Very High	High	Partial	Active
Indonesia	Emerging	Moderate–High	Weak	Moderate
Malaysia	Emerging	High	Weak	Limited
Myanmar	Low	Extreme	None	Suppressed
Nepal	Low–Emerging	High	Weak	Active
Pakistan	Emerging	High	Weak	Limited
Philippines	Emerging	Moderate	Partial	Active

Across the ten countries, four broad clusters emerge:

Cluster A - Meaningful safeguards with active civil society: Australia and the Philippines. Both have independent data protection or oversight bodies (OAIC and ACCC in Australia; the NPC in the Philippines) and active civil society organisations scrutinising DPI governance. Australia's governance model is stronger structurally; the Philippines shows how good institutions can be undermined by political context.

Cluster B - High DPI maturity with structural surveillance risk: India. India's DPI is technically the most advanced in this study, with near-universal biometric enrolment and massive payment infrastructure. Legal frameworks are developing but lag behind the infrastructure, and the gap between policy aspiration and implementation is significant.

Cluster C - Emerging DPI with accumulating governance risks: Bangladesh, Indonesia, Malaysia, Nepal, and Pakistan. These countries are building DPI rapidly while governance frameworks lag behind. Key risk factors include: biometric identity infrastructure without strong data protection (Indonesia, Pakistan); law enforcement integration without legal constraint (Malaysia, Pakistan); surveillance legislation outpacing data protection frameworks (Nepal, Bangladesh); and financial governance failures at the infrastructure level (Malaysia).

Cluster D - Authoritarian or conflict contexts with no meaningful safeguards: Afghanistan and Myanmar. In both cases, the political context renders rights-protective DPI governance impossible under current conditions. Digital infrastructure is an instrument of state control.

Cross-Cutting Observations

- Function creep is the dominant structural risk across the study. Almost every country faces the risk that data collected for service delivery will be repurposed for law enforcement, political monitoring, or commercial profiling. Australia is the only country whose governance model explicitly addresses this risk in its legislative architecture.
- Biometric identity systems amplify surveillance risk. Countries with facial recognition or fingerprint/iris biometrics in their digital identity layer (India, Indonesia, Bangladesh, and Pakistan) face higher structural risk because biometric data cannot be changed if misused and enables persistent identification across contexts.
- Law enforcement integration is an understudied risk factor. Malaysia's police integration, Pakistan's NADRA access for law enforcement, and the Philippines' SIM registration all illustrate how DPI becomes law enforcement infrastructure without being designed or governed as such.
- Civil society capacity is the clearest predictor of governance quality. Countries where civil society organisations can research, publicise, and advocate around surveillance risks (Australia, Philippines, India, and Nepal) show better governance outcomes than those where such capacity is suppressed (Myanmar and Afghanistan) or legally constrained (Bangladesh, Malaysia, and Pakistan).

- Breadth of digital security legislation correlates with suppression risk. Countries with broadly worded cybercrime or digital security legislation (Bangladesh, Pakistan, Nepal, and Myanmar) face compound risk: the legal tool for surveillance is the same tool used to criminalise criticism of surveillance.

Limitations

Most sources reviewed were in English. Domestic debates in Bangla, Bahasa Indonesia, Malay, Nepali, Burmese, Urdu, Tagalog, or Dari and Pashto are not captured in this interim review. This is a significant gap: civil society critique, parliamentary debate, and legal scholarship in local languages may substantially alter the picture for several countries.

Country coverage is uneven. India and Australia have robust English-language documentation. Afghanistan and Myanmar are extremely difficult to research, in Afghanistan due to Taliban control and collapse of independent media; in Myanmar due to the ongoing military junta. Bangladesh, Pakistan, and the Philippines have limited dedicated DPI-and-surveillance scholarship in English, though broader digital rights reporting exists.

References

Introduction

China Academy of Information and Communications Technology. (2025). Digital public infrastructure solutions: From the perspective of China's practices. http://www.caict.ac.cn/english/research/whitepapers/202509/P020250923335045699470.pdf

Digital Public Goods Alliance. (2024). Digital public infrastructure and digital public goods: Policy perspectives. https://www.digitalpublicgoods.net/

Eaves, D., & Rao, K. (2025). Digital public infrastructure: A framework for conceptualisation and measurement (IIPP Working Paper 2025-01). UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2025/jan/digital-public-infrastructure-framework-conceptualisation-and-measurement

India G20 Task Force on Digital Public Infrastructure for Economic Transformation, Financial Inclusion and Development. (2024). Report of India's G20 Task Force on Digital Public Infrastructure. Department of Economic Affairs, Government of India. https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf

Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). Digital public infrastructure and public value: What is "public" about DPI? UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi

United Nations Development Programme. (2023). Accelerating the SDGs through digital public infrastructure. https://www.undp.org/sites/g/files/zskgke326/files/2023-08/accelerating_the_sdgs_through_digital_public_infrastructure.pdf

World Bank. (2025). Digital public infrastructure and development: A World Bank Group approach. https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf

1. Stating Without Steering: National DPI Goals and the Accountability Gap Across Asia-Pacific States

Amir, S. K. (2026). Malaysia's approach to digital justice: Internet access as a human right. Open Global Rights. https://www.openglobalrights.org/malaysias-approach-to-digital-justice-internet-access-as-a-human-right/

Australian Government. (2025). 2025 digital ID rules and accreditation rules consultation: Redress framework. https://www.digitalidsystem.gov.au/have-your-say/2025-digital-id-rules-and-accreditation-rules-consultation

Australian Prudential Regulation Authority. (n.d.). Regulation impact statements. https://www.apra.gov.au/regulation-impact-statements

CAICT (China Academy of Information and Communications Technology). (2025). Digital public infrastructure solutions: From the perspective of China's practices. http://www.caict.ac.cn/english/research/whitepapers/202509/P020250923335045699470.pdf

Department of Information and Communications Technology, Papua New Guinea. (2025a). National digital ID policy 2025 (Draft version 7.2). https://www.ict.gov.pg/Draft%20Digital%20ID%20Policy/Draft%20Digital%20ID%20Policy%207.2%20-%2026%20June%2025.pdf

Department of Information and Communications Technology, Papua New Guinea. (2025b). Government digital ID standards, guidelines and specifications 2025. https://www.ict.gov.pg/Digital%20Standards/Government%20DIGITAL%20ID%20STANDARDS,%20GUIDELINES%20AND%20SPECS%202025%20.pdf

Digital Cooperation Organization. (2025). Bangladesh: Digital trade acceleration initiative. https://dco.org/wp-content/uploads/2025/10/Bangladesh-Report.pdf

Digital Transformation Agency. (2025). Major digital projects report: 2025. Australian Government. https://www.dta.gov.au/article/blog-release-major-digital-projects-report-2025

Eaves, D., & Rao, K. (2025). Digital public infrastructure: A framework for conceptualisation and measurement (IIPP WP 2025-01). UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2025/jan/digital-public-infrastructure-framework-conceptualisation-and-measurement

Economic Planning Unit, Prime Minister's Department, Malaysia. (2021). Malaysia digital economy blueprint. https://ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf

Flensburg, S., Lai, S., & Lehmann-Jacobsen, E. (2025). Digital infrastructures in Afghanistan. International Media Support. https://www.mediasupport.org/publication/digital-infrastructures-in-afghanistan/

Government of Pakistan. (2025). The digital nation Pakistan act, 2025. National Assembly of Pakistan. https://www.na.gov.pk/uploads/documents/679b239e8d57f_451.pdf

GovTech Developers Portal. (n.d.). Singpass. Government of Singapore. https://www.singpass.gov.sg/main/

IFEX. (2025). Myanmar junta builds a surveillance state. https://ifex.org/myanmar-junta-builds-a-surveillance-state/

India G20 Task Force on Digital Public Infrastructure for Economic Transformation, Financial Inclusion and Development. (2024). Report of India's G20 task force on digital public infrastructure. Department of Economic Affairs, Government of India. https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf

Kapur, A., & LaForge, G. (2026). Building open digital states: Country case studies on the impact of DPGs for DPI. Digital Public Goods Alliance. https://www.digitalpublicgoods.net/dpgs-for-dpi-building-open-digital-states.pdf

Liang, L. H. (2025). India pledges support for Myanmar digital ID pilot. Biometric Update. https://www.biometricupdate.com/202507/india-pledges-support-for-myanmar-digital-id-pilot

Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). Digital public infrastructure and public value: What is "public" about DPI? UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi

Ministry of Digital, Malaysia. (2025). Ministry of Digital to intensify RMK-13 initiatives. https://www.digital.gov.my/en-GB/siaran/Kementerian-Digital-Akan-Menggiatkan-Inisiatif-RMK-13

Ministry of Transport and Communications, Government of Myanmar. (2024). Myanmar e-governance master plan 2030. https://www.myanmar.gov.mm/documents/20143/0/Myanmar+e-Governance+Master+Plan+2030+(English+version).pdf

NASSCOM. (2024). Digital public infrastructure of India: Accelerating India's digital inclusion. https://new.nasscom.in/sites/default/files/publicreport/Digital%20Public%20Infrastructure%2022-2-2024_compressed.pdf

Nepal Rastra Bank. (2024). Payment systems oversight report 2023/24. https://www.nrb.org.np/contents/uploads/2025/01/Payment-Oversight-Report-2023-24.pdf

OECD. (2025). Digital government review of Korea. https://doi.org/10.1787/9defc197-en

OECD. (2025b). Enhancing digital investment in Australia. https://doi.org/10.1787/91c22326-en

Raihan, S., Prima, L. M., Surid, T. F., & Sharmin, E. (2025). The impact of digital public infrastructure (DPI) interventions on socioeconomic and development outcomes in Bangladesh (GDN Working Paper No. 97). Global Development Network. https://www.gdn.int/sites/default/files/WORKING%20PAPER%20no.%2097.pdf

Sarjito, A., & Thamrin, S. (2026). Digital governance reform in Indonesia: A comparative analysis with Estonia. Public Administration Issues. https://doi.org/10.17323/1999-5431-2026-0-5-92-116

Seth, A., Vitagliano, L. F., Udupa, N., Singh, P. J., Swamy, R., Singh, S., & Venugopal, V. (2023). A governance framework for digital public infrastructure: Learning from the Indian experience. T20 Policy Brief, Task Force 2. https://www.defindia.org/wp-content/uploads/2023/07/T20_PB_TF2_205_DPI-Indian-Experience.pdf

Statelessness Encyclopaedia Asia Pacific. (2025). Afghanistan. https://seap.nationalityforall.org/digital-id/regional-overview/south-asia/afghanistan/

United Nations Development Programme. (2023). Accelerating the SDGs through digital public infrastructure. https://www.undp.org/sites/g/files/zskgke326/files/2023-08/accelerating_the_sdgs_through_digital_public_infrastructure.pdf

World Bank. (2025a). Digital public infrastructure and development: A World Bank Group approach. https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf

World Bank. (2025b). Implementation status and results report: Islamic Republic of Pakistan digital economy enhancement project (Sequence No. 2).

https://documents1.worldbank.org/curated/en/099011525100510857/pdf/P174402-c583176c-1d59-45ef-a8f4-a906c8730eca.pdf

World Bank. (2025c). Islamic Republic of Pakistan: Digital economy enhancement project — project information document (Appraisal stage). https://documents1.worldbank.org/curated/en/099455001172320746/pdf/P1744020453111c010b4e10ea4415c52d4a.pdf

World Bank & GovTech Singapore. (2022). National digital identity and government data sharing in Singapore: A case study of Singpass and APEX. https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf

2. How Is Digital Public Infrastructure Defined? Legal Recognition Across the Asia-Pacific

Australian Government. (2024). *Digital ID Act 2024* (Act No. 25, 2024). Federal Register of Legislation. https://www.legislation.gov.au/C2024A00025/latest

Aspire to Innovate. (2022). *Smart Bangladesh Vision 2041*. ICT Division; UNDP Bangladesh. https://a2i.gov.bd/a2i-missions/smart-bangladesh-vision-2041/

Chaudhuri, R. (2023, September 1). *Decoding the G20 consensus on digital public infrastructure: A key outcome of India's presidency*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/09/decoding-the-g20-consensus-on-digital-public-infrastructure-a-key-outcome-of-indias-presidency

Central Committee of the Communist Party of China, & The State Council of The People' Republic of China. (2023, February 27). Overall Layout Plan for the Construction of Digital China. https://www.gov.cn/zhengce/2023-02/27/content_5743484.html

Department of Information and Communications Technology. (2025). *About SevisPNG: Papua New Guinea's digital identity ecosystem*. Government of Papua New Guinea. https://www.sevis.gov.pg/about

Digital Public Goods Alliance. (2022, May 17). *Unpacking concepts & definitions: Digital public infrastructure, building blocks, and their relation to digital public goods*. https://www.digitalpublicgoods.net/blog/unpacking-concepts-definitions-digital-public-infrastructure-building-blocks-and-their-relation-to-digital-public-goods

Economic Planning Unit. (2021). *Malaysia Digital Economy Blueprint*. Ministry of Economy, Malaysia. https://ekonomi.gov.my/en/resources/publications/malaysia-digital-economy-blueprint

Government of Indonesia. (2023). *Presidential Regulation No. 82 of 2023 on acceleration of digital transformation and integration of national digital services*. https://jdih.kemenkeu.go.id/dok/perpres-82-tahun-2023

Government of Pakistan. (2025). *Digital Nation Pakistan Act 2025* (Act No. I of 2025). https://www.pakistancode.gov.pk/

Government of Papua New Guinea. (2022). *Digital Government Act 2022*. Department of Information and Communication Technology. https://www.ict.gov.pg/digital-government-act-2022/

Government of the Philippines. (2018). *Philippine Identification System Act* (Republic Act No. 11055). https://lawphil.net/statutes/repacts/ra2018/ra_11055_2018.htm

Government of the Philippines. (2025). *E-Governance Act* (Republic Act No. 12254). https://lawphil.net/statutes/repacts/ra2025/ra_12254_2025.html

Government of the Republic of Korea. (2020). *Framework Act on Intelligent Informatization*. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=69463&type=part&key=43

Hoffman, S., & Feldstein, S. (2026, March). *The architecture of digital repression*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2026/03/the-architecture-of-digital-repression

India G20 Task Force on Digital Public Infrastructure. (2024). *Report of India's G20 Task Force on Digital Public Infrastructure*. Government of India. https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf

Ministry of Communication and Information Technology. (2025). *Digital Nepal framework 2.0: A step towards a digitally empowered Nepal*. Government of Nepal. https://www.slideshare.net/slideshow/digital-nepal-framework-2-0-a-step-towards-a-digitally-empowered-nepal/277193454

Ministry of Communication and Information Technology. (2019). *Digital Nepal framework: Unlocking Nepal's growth potential*. Government of Nepal. https://www.digitaldevelopment.org/library/digital-nepal-framework/

Ministry of Economy. (2024). *Pangkalan Data Utama (PADU)* [Data initiative]. Government of Malaysia. https://padu.gov.my/

Organisation for Economic Co-operation and Development. (2024). *Digital government and public infrastructure governance*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf

Shires, J., & Wilkinson, I. (2024). *The internet under attack: Insights from Afghanistan and Ukraine on maintaining a resilient internet in conflict and crisis*. Chatham House. https://doi.org/10.55317/9781784136123

Smart Nation and Digital Government Group. (2018). *Digital government blueprint: A Singapore Government that is digital to the core and serves with heart*. Government of Singapore. https://www.tech.gov.sg/digital-government-blueprint/

Smith, G., & Russell, R. (2024, October 30). *Understanding digital government part 2: Digital public infrastructure*. United Nations Development Programme. https://www.undp.org/trinidad-and-tobago/blog/understanding-digital-government-part-2-digital-public-infrastructure

State Administration Council. (2025, January 1). *Cybersecurity law (State Administration Council Law No. 1/2025)*. https://www.icnl.org/resources/library/cybersecurity-law-state-administration-council-law-no-1-2025

United Nations Development Programme. (2023). *Accelerating the SDGs through digital public infrastructure: A compendium of the potential of digital public infrastructure*. https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure

World Bank. (2026). *Myanmar digital sector monitoring note*. World Bank Group Open Knowledge Repository. https://openknowledge.worldbank.org/entities/publication/93d753e4-446b-4747-8211-a72a896d622

World Bank. (2022). *National Digital Identity and government data sharing in Singapore: A case study of Singpass and APEX*. World Bank Group. https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf

3. Who Oversees DPI and On What Legal Authority? Legal Foundations and Oversight Bodies Across the Asia-Pacific

China Academy of Information and Communications Technology. (2025). Digital public infrastructure solutions: From the perspective of China's practices. http://www.caict.ac.cn/english/research/whitepapers/202509/P020250923335045699470.pdf

Data Privacy Act of 2012, Republic Act No. 10173 (Philippines). https://privacy.gov.ph/data-privacy-act/

Department of Information and Communications Technology, Papua New Guinea. (2025). Government digital ID standards, guidelines and specifications 2025. https://www.ict.gov.pg/Digital%20Standards/Government%20DIGITAL%20ID%20STANDARDS,%20GUIDELINES%20AND%20SPECS%202025%20.pdf

Digital Cooperation Organization. (2025). Bangladesh: Digital trade acceleration initiative report. https://dco.org/wp-content/uploads/2025/10/Bangladesh-Report.pdf

Eaves, D., & Rao, K. (2025). Digital public infrastructure: A framework for conceptualisation and measurement (IIPP WP 2025-01). UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2025/jan/digital-public-infrastructure-framework-conceptualisation-and-measurement

E-Governance Act, Republic Act No. 12254 (2025) (Philippines). https://www.lawphil.net/statutes/repacts/ra2025/ra_12254_2025.html

European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Flensburg, S., Lai, S., & Lehmann-Jacobsen, E. (2025). Digital infrastructures in Afghanistan. International Media Support. https://www.mediasupport.org/publication/digital-infrastructures-in-afghanistan/

Government of Bangladesh. (2025). Personal Data Protection Ordinance, 2025 (Ordinance No. 61 of 2025). https://www.dpp.gov.bd/upload_file/gazettes/59177_96371.pdf

Government of Pakistan. (2025). Digital Nation Pakistan Act, 2025 (Act No. I of 2025). National Assembly of Pakistan. https://www.na.gov.pk/uploads/documents/679b239e8d57f_451.pdf

GovTech Singapore. (2022). National digital identity and government data sharing in Singapore: A case study. https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf

IIM Bangalore, & Protean. (2025). State of DPI in India. Indian Institute of Management Bangalore. https://www.iimb.ac.in/cdpg/pdf/State-India-DPI_Report.pdf

India G20 Task Force on Digital Public Infrastructure for Economic Transformation, Financial Inclusion and Development. (2024). Report of India's G20 Task Force on Digital Public Infrastructure. Department of Economic Affairs, Government of India. https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf

International Comparative Legal Guides. (2025). Data protection laws and regulations report 2025–2026: Pakistan. Global Legal Group. https://iclg.com/practice-areas/data-protection-laws-and-regulations/pakistan

Kapur, A., & LaForge, G. (2026). Building open digital states: Country case studies on the impact of DPGs for DPI. Digital Public Goods Alliance. https://www.digitalpublicgoods.net/dpgs-for-dpi-building-open-digital-states.pdf

Ministry of Digital, Malaysia. (2025). Ministry of Digital to intensify RMK-13 initiatives. https://www.digital.gov.my/en-GB/siaran/Kementerian-Digital-Akan-Menggiatkan-Inisiatif-RMK-13

Ministry of Electronics and Information Technology [India]. (2023). Digital Personal Data Protection Act, 2023. Government of India. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Ministry of Electronics and Information Technology [India]. (2025). Digital Personal Data Protection Rules, 2025. Government of India. https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

Ministry of Electronics and Information Technology [India]. (2026). Appointment to the post of Chairperson and Other Members in the Data Protection Board of India (F. No. 2(1)/2026-Pers.I, 6 May 2026). Government of India. https://www.meity.gov.in/static/uploads/2026/05/cd481c027470b420b4cb85fb40a91c53.pdf

Ministry of Transport and Communications, Government of Myanmar. (2024). Myanmar e-governance master plan 2030.

https://www.myanmar.gov.mm/documents/20143/0/Myanmar+e-Governance+Master+Plan+2030+(English+version).pdf

Nepal Rastra Bank. (2025). Payment systems oversight report 2023/24. https://www.nrb.org.np/contents/uploads/2025/01/Payment-Oversight-Report-2023-24.pdf

Organisation for Economic Co-operation and Development. (2025a). Digital government in Australia: Enhancing digital investment. OECD Publishing. https://doi.org/10.1787/91c22326-en

Organisation for Economic Co-operation and Development. (2025b). Digital government review of Korea. OECD Publishing. https://doi.org/10.1787/9defc197-en

Personal Data Protection Act 2012, No. 26 of 2012 (Singapore). Singapore Statutes Online, Attorney-General's Chambers. https://sso.agc.gov.sg/Act/PDPA2012

Philippine Identification System Act, Republic Act No. 11055 (2018) (Philippines). https://philsys.gov.ph/wp-content/uploads/2024/09/RA11055-REVISED-IRR.pdf

Public Sector (Governance) Act 2018 (Singapore). Singapore Statutes Online, Attorney-General's Chambers. https://sso.agc.gov.sg/Act/PSGA2018

Sarjito, A., & Thamrin, S. (2026). Digital governance reform in Indonesia: A comparative analysis with Estonia. Public Administration Issues, (5), 92–116. https://doi.org/10.17323/1999-5431-2026-0-5-92-116

Shires, J., & Wilkinson, I. (2024). The internet under attack: Insights from Afghanistan and Ukraine on maintaining a resilient internet (Chapter 3). Chatham House. https://www.chathamhouse.org/2024/08/internet-under-attack/03-internet-resilience-afghanistan

United Nations Development Programme. (2023). Accelerating the SDGs through digital public infrastructure. https://www.undp.org/sites/g/files/zskgke326/files/2023-08/accelerating_the_sdgs_through_digital_public_infrastructure.pdf

United Nations General Assembly. (2024). Resolution 79/1: Pact for the Future (including the Global Digital Compact). United Nations. https://digitallibrary.un.org/record/4061879?ln=en&v=pdf

World Bank. (2023). Islamic Republic of Pakistan: Digital economy enhancement project, project information document (Appraisal stage). World Bank Group.

https://documents1.worldbank.org/curated/en/099455001172320746/pdf/P174402045311c010b4e10ea4415c52d4a.pdf

World Bank. (2025a). Digital public infrastructure and development: A World Bank Group approach. https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf

World Bank. (2025b). Implementation status and results report: Islamic Republic of Pakistan digital economy enhancement project (P174402), Sequence No. 2. https://documents1.worldbank.org/curated/en/099011525100510857/pdf/P174402-c583176c-1d59-45ef-a8f4-a906c8730eca.pdf

4. Who Shapes DPI in APAC? A Comparative Study of Consultation Practices in DPI Governance

Access Now. (2024). *A human rights-centered approach to digital public infrastructure: Safeguarding civil society in restrictive environments*. https://www.accessnow.org/guide/digital-public-infrastructure/

AfricLaw. (2026, February 11). *Digital public infrastructure through an open government lens*. https://africlaw.com/2026/02/11/digital-public-infrastructure-through-an-open-government-lens/

Bank Indonesia. (2019). *Blueprint sistem pembayaran Indonesia 2025: Menavigasi sistem pembayaran nasional di era digital* [Indonesia payment system blueprint 2025: Navigating the national payment system in the digital era].https://openresearch-repository.anu.edu.au/bitstream/1885/277124/1/IndoCorp_55.pdf

Department of Information and Communications Technology. (2025). *Digital ID Policy: National Digital ID Policy 2025*. Government of Papua New Guinea. https://www.ict.gov.pg/digital-id-policy/

Department of Information and Communications Technology. (2026). *DICT releases draft national sovereign digital transformation and AI strategy for public consultation*. Government of Papua New Guinea. https://www.ict.gov.pg/png-releases-draft-national-sovereign-digital-transformation-and-ai-strategy-for-public-consultation/

Digital Rights Foundation. (2023). *Policy submission and civil society assessment on the personal data protection bill: Human rights in the digital age*. https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf

Eaves, D., & Rao, K. (2025). *Digital Public Infrastructure: A framework for conceptualisation and measurement* (IIPP WP 2025-01). UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2025/jan/digital-public-infrastructure-framework-conceptualisation-and-measurement

Economic Planning Unit. (2021). *Malaysia digital economy blueprint*. Prime Minister's Department, Government of Malaysia. https://ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf

Freedom House. (2024). *Myanmar: Freedom on the net 2024 country report*.https://freedomhouse.org/country/myanmar/freedom-net/2024

Global Digital Public Infrastructure Repository. (n.d.). *Global DPIs*. https://www.dpi.global/home

Goggin, G., Vromen, A., Weatherall, K., Martin, F., & Sunman, L. (2019). Data and digital rights: Recent Australian developments. *Internet Policy Review*, *8*(1), 1–19. https://doi.org/10.14763/2019.1.1390

Maheshwari, D. & Sharma, B. (2025). *Governing Digital India: A report on institutions and instruments*. Centre for Social and Economic Progress. https://csep.org/wp-content/uploads/2025/10/GOVERNING-DIGITAL-INDIA.pdf

Nepal Digital Transformation Project. (2025). *Stakeholder Engagement Plan*. https://giwmscdntwo.gov.np/media/pdf_upload/stakeho_hmop3rk.pdf

Organisation for Economic Co-operation and Development. (2017). *Regulatory policy in Korea: Towards better regulation*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/05/regulatory-policy-in-korea_g1g7912e/9789264274600-en.pdf

Seth, A., Vitagliano, L. F., Udupa, N., Singh, P. J., Swamy, R., Singh, S., & Venugopal, V. (2023, July). *A governance framework for digital public infrastructure: Learning from the Indian experience*. https://www.defindia.org/wp-content/uploads/2023/07/T20_PB_TF2_205_DPI-Indian-Experience.pdf

Statelessness Encyclopedia Asia Pacific - SEAP (2025, August 15). *Afghanistan*. https://seap.nationalityforall.org/digital-id/regional-overview/south-asia/afghanistan/

UNDP. (n.d.). *Digital public infrastructure (DPI)*. https://www.undp.org/digital/digital-public-infrastructure

United Nations Office for Digital and Emerging Technologies, & United Nations Development Programme. (2024). *Universal DPI safeguards framework*. DPI Safeguards. https://www.dpi-safeguards.org/framework

World Bank. (2022). *National digital identity and government data sharing in Singapore: A case study of Singpass and APEX*. https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf

5. Who Can Citizens Turn To? Accountability Through Grievance Redress and Transparency in Asia-Pacific Digital Public Infrastructure

Ahmed, O. N. (2025, December 11). Data privacy in peril: Pakistan's legal vacuum and its consequences. *The Friday Times.* https://www.thefridaytimes.com/11-Dec-2025/data-privacy-peril-pakistan-s-legal-vacuum-consequences

Association of Banks in Singapore. (n.d.). *PayNow Singapore.* https://www.abs.org.sg/e-payments/pay-now

Bachtiar, G. (2025). Embedding ethical AI in digital public infrastructure: Strategic governance pathways for Indonesia. *Journal of Indonesian Policy and Management, 8*(2). https://doi.org/10.35166/jipm.v8i2.123

Department of Information and Communications Technology, Papua New Guinea. (n.d.). *National Digital ID Policy 2025, draft version 7.2.* https://www.ict.gov.pg/Draft%20Digital%20ID%20Policy/Draft%20Digital%20ID%20Policy%207.2%20-%2026%20June%2025.pdf

Digital Rights Foundation. (2023). *Legal analysis and statement on the Personal Data Protection Bill, 2023.* https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf

Eaves, D., & Rao, K. (2025). *Digital public infrastructure: A framework for conceptualisation and measurement* (IIPP Working Paper 2025-01). UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2025/jan/digital-public-infrastructure-framework-conceptualisation-and-measurement

European Parliament and Council. (2016, April 27). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union.* https://eur-lex.europa.eu/eli/reg/2016/679/oj

Flensburg, S., Lai, S., & Lehmann-Jacobsen, E. (2025). *Digital infrastructures in Afghanistan.* International Media Support. https://www.mediasupport.org/publication/digital-infrastructures-in-afghanistan/

Gobind Singh Deo, Minister of Digital. (2025). *Ministry of Digital to intensify RMK-13 initiatives.* Office of the Minister, Ministry of Digital, Malaysia. https://www.digital.gov.my/en-GB/siaran/Kementerian-Digital-Akan-Menggiatkan-Inisiatif-RMK-13

Government of India. (n.d.). *Global Digital Public Infrastructure Repository.* https://www.dpi.global/home

Government of Pakistan. (2025, January 29). *The Digital Nation Pakistan Act, Act No. I of 2025.* National Assembly of Pakistan. https://www.na.gov.pk/uploads/documents/679b239e8d57f_451.pdf

Government of Singapore. (2012). *Personal Data Protection Act 2012, No. 26 of 2012.* Singapore Statutes Online, Attorney-General's Chambers. https://sso.agc.gov.sg/Act/PDPA2012

Government of Singapore. (2018). *Public Sector (Governance) Act 2018.* Singapore Statutes Online, Attorney-General's Chambers. https://sso.agc.gov.sg/Act/PSGA2018

GovTech Developers Portal. (n.d.). *Singpass.* https://www.singpass.gov.sg/main/

International Comparative Legal Guides. (2025). *Data protection laws and regulations report 2025 to 2026: Pakistan.* Global Legal Group. https://iclg.com/practice-areas/data-protection-laws-and-regulations/pakistan

Kapur, A., & LaForge, G. (2026). *Building open digital states: Country case studies on the impact of DPGs for DPI.* Digital Public Goods Alliance. https://www.digitalpublicgoods.net/dpgs-for-dpi-building-open-digital-states.pdf

Library of Congress. (2018, July 19). Afghanistan: Distribution of controversial electronic identity cards launched. *Global Legal Monitor.* https://www.loc.gov/item/global-legal-monitor/2018-07-19/afghanistan-distribution-of-controversial-electronic-identity-cards-launched/

Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). *Digital public infrastructure and public value: What is public about DPI?* UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi

Ministry of Information Technology and Telecommunication, Government of Pakistan. (2023, May). *Personal Data Protection Bill, 2023: Final draft.* https://www.icnl.org/wp-content/uploads/Personal-Data-Protection-Bill-2023.pdf

NASSCOM. (2024, February 1). *Digital public infrastructure of India - Accelerating India's digital inclusion*. https://new.nasscom.in/sites/default/files/publicreport/Digital%20Public%20Infrastructure%2022-2-2024_compressed.pdf

Nieborg, D. B. (n.d.). On super apps and app stores: Digital media logics in China's app economy. *Media, Culture and Society.* https://www.academia.edu/88798103/On_super_apps_and_app_stores_digital_media_logics_in_Chinas_app_economy

Organisation for Economic Co-operation and Development. (2025). *Digital Government Review of Korea.* OECD Publishing. https://doi.org/10.1787/9defc197-en

Raihan, S., Prima, L. M., Surid, T. F., & Sharmin, E. (2025). *The impact of digital public infrastructure (DPI) interventions on socioeconomic and development outcomes in Bangladesh* (Working Paper No. 97). Global Development Network. https://www.gdn.int/sites/default/files/WORKING%20PAPER%20no.%2097.pdf

Seth, A., Vitagliano, L. F., Udupa, N., Singh, P. J., Swamy, R., Singh, S., & Venugopal, V. (2023). *A governance framework for digital public infrastructure: Learning from the Indian experience.* T20 Policy Brief. https://www.defindia.org/wp-content/uploads/2023/07/T20_PB_TF2_205_DPI-Indian-Experience.pdf

Shires, J., & Wilkinson, I. (2024, August). *The internet under attack: Insights from Afghanistan and Ukraine on maintaining a resilient internet* (Chapter 3). Chatham House. https://www.chathamhouse.org/2024/08/internet-under-attack/03-internet-resilience-afghanistan

Statelessness Encyclopaedia Asia Pacific. (2025). *Afghanistan.* https://seap.nationalityforall.org/digital-id/regional-overview/south-asia/afghanistan/

United Nations Development Programme. (2023). *Accelerating the SDGs through digital public infrastructure.* https://www.undp.org/sites/g/files/zskgke326/files/2023-08/accelerating_the_sdgs_through_digital_public_infrastructure.pdf

World Bank. (2023). *Islamic Republic of Pakistan: Digital Economy Enhancement Project, Project Information Document (Appraisal Stage).* World Bank Group. https://documents1.worldbank.org/curated/en/099455001172320746/pdf/P1744020453111c010b4e10ea4415c52d4a.pdf

World Bank. (2025a). *Digital public infrastructure and development: A World Bank Group approach.* World Bank Group. https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf

World Bank. (2025b). *Implementation Status and Results Report: Islamic Republic of Pakistan Digital Economy Enhancement Project (P174402), Sequence No. 2.* World Bank Group.

https://documents1.worldbank.org/curated/en/099011525100510857/pdf/P174402-c583176c-1d59-45ef-a8f4-a906c8730eca.pdf

World Bank, & Government Technology Agency of Singapore. (2022). *National digital identity and government data sharing in Singapore: A case study of Singpass and APEX*. World Bank. https://openknowledge.worldbank.org/handle/10986/37452

World Bank. (2022). *Using biometrics to deliver cash payments to women: Early results from an impact evaluation in Pakistan* (Report No. P176341). https://documents1.worldbank.org/curated/en/099155004142238180/pdf/P1763410d1e1af00108e170e5754d04fed9.pdf

Yang, Y. (2023). SoK: Decoding the super app enigma: The security mechanisms, threats, and trade-offs in OS-alike apps. *ArXiv.* https://arxiv.org/pdf/2306.07495

Zeng, M., & Kim, Y. (2025). Institutional reforms and regulatory shifts in China's digital platform sector: How domain-specific centralization shaped the 2020-2022 transition. *Business and Politics.* https://doi.org/10.1017/bap.2025.10015

6. Serving or Surveilling? Surveillance Risk and Civil Society Oversight in Asia-Pacific DPI

Amnesty International. (2024). *Repackaging Repression: The Cyber Security Act.* https://www.amnesty.org.au/wp-content/uploads/2024/08/Bangladesh-Cyber-Security-Act-Report.pdf

Amnesty International. (2025). *Pakistan: authorities pass bill with sweeping controls on social media*. https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/

Access Now. (2025). *Myanmar's digital dictatorship*. https://www.accessnow.org/myanmar/

Article 19. (2022). *Philippines SIM Card Registration Act undermines online freedoms.* https://www.article19.org/resources/philippines-sim-card-registration-act-undermines-online-freedoms/

Article 19. (2023). *UN: Ongoing digital dictatorship in Myanmar*. https://www.article19.org/resources/un-ongoing-digital-dictatorship-in-myanmar/

Australian Government. (2024). *Digital ID Act 2024.* Commonwealth of Australia. https://www.legislation.gov.au

Biometric Update. (2026). *Audit finds spending and governance failures in Malaysia's MyDigital ID*. https://www.biometricupdate.com/202602/audit-finds-spending-and-governance-failures-in-malaysias-mydigital-id

Biometric Update. (2025). *Malaysia begins MyDigital ID verification integration for all mobile operators*. https://www.biometricupdate.com/202512/malaysia-begins-mydigital-id-verification-integration-for-all-mobile-operators

Biometric Update. (2026). *Philippines social media identity verification proposal draws rights criticism.* https://www.biometricupdate.com/202602/philippines-social-media-identity-verification-proposal-draws-rights-criticism

Biometric Update. (2025). *The next five years of DPI in Indonesia will reshape lives: IFIS 2025 panel.* https://www.biometricupdate.com/202505/the-next-five-years-of-dpi-in-indonesia-will-reshape-lives-ifis-2025-panel

CIVICUS Monitor. (2025). *Pakistan: activists and journalists targeted*. https://monitor.civicus.org/explore/pakistan-activists-and-journalists-targeted-increased-controls-on-online-expression-and-crackdown-on-protests/

Comparitech. (2024). *Digital IDs study: How countries compare on digital identity systems.* Comparitech. https://www.comparitech.com/blog/vpn-privacy/digital-ids-study/

CPA Australia. (2025). *Digital ID, age verification, eSafety laws: what you need to know.* https://cpa.org.au/guardian/issue-2163/digital-id-age-verification-esafety-laws-what-you-need-to-know/

CSIS. (2024). *Approaches to digital public infrastructure in the Global South.* Center for Strategic and International Studies. https://www.csis.org/analysis/approaches-digital-public-infrastructure-global-south

CSIS. (2025). *Ten years of UPI: Implications of India's digital public infrastructure*. Center for Strategic and International Studies. https://www.csis.org/blogs/strategic-technologies-blog/ten-years-upi-implications-indias-digital-public-infrastructure

Datareportal. (2026). *Global digital overview 2026.* DataReportal. https://datareportal.com/global-digital-overview

Digital Freedom Network Philippines. (2026). *Data privacy and the Philippine Identification System*. https://digitalfreedom.ph/data-privacy-and-the-philippine-identification-system/

Digital Rights Nepal. (2025). *The state of digital rights and safety in Nepal 2025.* Digital Rights Nepal. https://digitalrightsnepal.org/report/the-state-of-digital-rights-and-safety-in-nepal-2025/

Electronic Frontier Foundation. (2009). *Surveillance self-defense: International.* EFF. https://www.eff.org/wp/surveillance-self-defense-international

Factually.co. (2025, December). *Australia's national digital ID protests main complaints*. https://factually.co/fact-checks/politics/australia-national-digital-id-protests-main-complaints-d06393

Freedom House. (2024). *Freedom on the Net 2024: Myanmar*. https://freedomhouse.org/country/myanmar/freedom-net/2024

Freedom Online Coalition. (2023). *Guiding principles on government use of surveillance technologies.* Freedom Online Coalition. https://freedomonlinecoalition.com/guiding-principles-on-government-use-of-surveillance-technologies/

Gandy, O. H. (1993). *The panoptic sort: A political economy of personal information.* Westview Press. http://truthcloud.net/truthcloud/networks/the-panoptic-sort.pdf

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2022). *Surveillance.* Internet Policy Review. https://policyreview.info/concepts/surveillance

Human Rights Myanmar. (2025). *Privacy violations and discrimination in Myanmar*. https://humanrightsmyanmar.org/privacy-violations-and-discrimination-in-myanmar/

ICLG. (2025). *Data protection laws and regulations: Indonesia.* https://iclg.com/practice-areas/data-protection-laws-and-regulations/indonesia/

IMS (International Media Support). (2025). *Digital infrastructures in Afghanistan.* IMS. https://www.mediasupport.org/wp-content/uploads/2025/03/Digital_Infrastructres_Afghanistan_IMS.pdf

India Stack / exclusion documentation. (2026). *Human cost of India Stack.* https://indiastack.in/exclusion/

Legal Information Institute. (2021). *Surveillance.* Cornell Law School. https://www.law.cornell.edu/wex/surveillance

Malaysia4U. (2026). *MyDigital ID Malaysia guide 2026*. https://malaysia4u.com/mydigital-id-guide

MediaNama. (2025). *What Nepal's social media ban means for digital speech rights*. https://www.medianama.com/2025/09/223-nepal-social-media-ban-digital-speech-rights-impact-safe-harbor-user-anonymity/

Nepal Explained. (2025). *Nepal's surveillance build-out explained.* Nepal Explained. https://nepalexplained.substack.com/p/nepals-surveillance-build-out-explained

NPR. (2018). *India's biometric ID system has led to starvation for some poor.* https://www.npr.org/2018/10/01/652513097/indias-biometric-id-system-has-led-to-starvation-for-some-poor-advocates-say

OHCHR. (2023). *Bangladesh: Türk urges immediate suspension of Digital Security Act.* https://www.ohchr.org/en/press-releases/2023/03/bangladesh-turk-urges-immediate-suspension-digital-security-act-media

Rethink Aadhaar. (2025). *A warning on India's biometric identity model*. https://rethinkaadhaar.in/blog/2025/10/24/a-warning-on-indias-biometric-identity-model

Richards, N. M. (2013). *The dangers of surveillance. Harvard Law Review*, *126*(7), 1934–1965. https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/

RSF. (2025). *Pakistan: multiple journalists and a dozen YouTube channels targeted under PECA*. https://rsf.org/en/pakistan-multiple-journalists-and-dozen-youtube-channels-targeted-under-peca-less-year

Salsa Digital. (2026). *Australia's Digital ID System, 2024 update.* https://salsa.digital/insights/australias-digital-id-system-2024-update

Springer / IJPCS. (2024). *Contestations of internet governance and digital authoritarianism in Pakistan*. https://link.springer.com/article/10.1007/s10767-024-09493-2

S.S. Rana & Co. (2025). *Nepal blocks 26 social media platforms in historic ban*. https://ssrana.in/articles/nepal-blocks-26-social-media-platforms-in-historic-ban/

Swiss German University. (2025). *How Indonesia's UU PDP 2022 shapes cybersecurity readiness in 2025.* https://sgu.ac.id/uu-pdp-2022-indonesia-cybersecurity-readiness-2025/

Tech Policy Press. (2024). *India's digital infrastructure is going global: What kind of power is it building?* Tech Policy Press. https://www.techpolicy.press/indias-digital-infrastructure-is-going-global-what-kind-of-power-is-it-building/

Tech Policy Press. (2025). *Fourth year under Myanmar military's digital iron curtain*. https://www.techpolicy.press/fourth-year-under-myanmar-militarys-digital-iron-curtain-a-reflection-on-digital-repression-and-the-path-forward/

The Edge Malaysia. (2026). *Mimos spent RM28 mil without relevant approvals, AG's Report*. https://theedgemalaysia.com/node/793596

Tribune Pakistan. (2025). *NADRA unveils new rules to strengthen digital ID system*. https://tribune.com.pk/story/2572883/nadra-unveils-new-rules-to-strengthen-digital-id-system

Wikipedia. (2025). *Digital Personal Data Protection Rules, 2025*. https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Rules,_2025

World Bank. (2026). *Global digital public infrastructure program*. https://www.worldbank.org/en/results/2026/05/06/global-digital-public-infrastructure-program