From Risk to Resilience: A Rights-based Approach to Digital Public Infrastructure (DPI) Readiness in the Global Majority

Discussion Paper

16 July 2025

RightsCon25

The Quantum Hub (TQH), in collaboration with Access Now and the National Institute of Strategic Resilience (NISR), Australia, co-organised a closed-door satellite workshop at RightsCon 2025, the most recent edition of the world's leading summit on human rights in the digital age. The workshop was titled:

"From Risk to Resilience:
A Rights-based Approach to Digital Public Infrastructure (DPI) Readiness in the Global Majority"

About the organisers

The Quantum Hub (TQH), India

The Quantum Hub (TQH) is a leading public policy research and communications firm based in New Delhi, India. Its work spans the domains of technology and social policy, with a focus on generating evidence-based insights to inform and influence public discourse and policymaking. TQH collaborates with a wide range of stakeholders, including leading technology companies, multilateral organisations, philanthropic foundations, and governments.

National Institute of Strategic Resilience (NISR), Australia

The National Institute of Strategic Resilience (NISR) is a non-partisan, not-for-profit research organisation in Canberra, Australia. A collaboration of senior leaders from industry, academia, the military, and government, NISR delivers fresh insights on strategic resilience, public policy, and security challenges. It advances thinking in these areas by applying diverse social lenses to better understand the opportunities and risks facing Australia, the Indo-Pacific, and the global community.

Access Now

Founded in 2009, Access Now defends and extends the digital rights of people and communities at risk. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age. Access Now is made up of a diverse community of more than 130 team members across five continents, working in centers of political power, tech innovation, and civic action around the world.

About RightsCon

RightsCon is the world's leading summit on human rights in the digital age. A space for a global, multi-stakeholder community of activists, technologists, policymakers, business leaders, journalists, philanthropists, researchers, and artists to connect, collaborate, and drive change on the most pressing issues at the intersection of human rights and technology.

For its 13th edition, RightsCon 2025 took place in Taipei, Taiwan and online from February 24 to February 27. We are incredibly grateful to Access Now for organising and spearheading this international convening.

Table of Contents

Introduction: Session Context and Objectives

Digital Public Infrastructures (DPIs) offer immense opportunities to enhance social and economic inclusion through digital transformation. However, when DPI adoption is not adequately assessed in terms of "readiness" and "risks", it can exacerbate marginalization, inaccessibility, surveillance, digital divides, concentration of control, and negatively impact people's human rights. DPIs have the potential to accelerate progress towards UN Sustainable Development Goals (SDGs), such as SDG 1 (No Poverty), SDG 3 (Good Health & Well-being), and SDG 5 (Gender Equality), among others.[1] To fulfill this promise, countries and communities deploying DPIs must be equipped with readiness frameworks to anticipate and mitigate risks effectively.

The Quantum Hub (TQH), India, and the **National Institute of Strategic Resilience (NISR)**, **Australia**, are collaborating to develop DPI adoption roadmaps that facilitate inclusive adoption across the global majority, including some lower-middle-income countries (LMICs). **Access Now** champions a human rights-centered approach to DPIs through its cross-regional advocacy. In this context, a **closed-door satellite workshop, co-organised by TQH, NISR, and Access Now**, was recently held at RightsCon 2025, the most recent edition of the world's leading summit on human rights in the digital age. It convened a diverse group of experts across civil society, industry, academia, multilateral organizations, etc. to:

- Facilitate shared understandings of risks that may arise when adopting DPIs in the global majority LMICs;
- Identify suitable safeguards and interventions that proactively mitigate various risks;
- Elicit critical questions that can generate healthy public debates on DPI deployment; and
- Co-create actionable playbooks that help countries evaluate DPI readiness and promote rights-respecting digital transformation.

The context for the proceedings was set through the following opening interventions:

Opening Address **Carolyn Tackett, Campaigns & Rapid Response Director, Access Now**	In this address, Ms Tackett underscored the significance of the theme of this workshop, given DPI's potential for great benefits and its implications for human rights if poorly designed and implemented. She stated that **activists and technologists have been highlighting the importance of reliable, accessible, equitable, sustainable, and decentralised digital infrastructure for decades, but much of the focus is centered on economic advancement and private sector growth, without adequate emphasis on community-led innovation that fosters civic engagement.**

[1] "Accelerating the SDGs through Digital Public Infrastructure: A Compendium of the Potential of Digital Public Infrastructure." UNDP, n.d. https://drive.google.com/file/d/1y-IUwq7iZbG-1Y6bdaZHWvKl94x4ikpe/view?usp=drive_link. For more details on how DPIs across the world are contributing to SDGs, please see this report.

	Ms Tackett also highlighted that the baseline assumption that DPIs need a foundational layer of digital legal identity, along with mechanisms for digital payments and streamlined data transfer, is, on one hand, too narrow and on the other hand, too broad. This is because **decision makers are unable to adequately contend with the realities of offline infrastructures and human rights considerations associated with the aforementioned three layers**. She suggested relying on the lessons learnt and progress made so far, and advocated for a human rights-centered approach to DPI that enables tailored, community-driven systems.
Technical Presentation **Professor David Watts, on behalf of the National Institute of Strategic Resilience**	Professor Watts highlighted that the definition of DPI remains amorphous and lacks consensus, but emerging consensus exists on **core DPI elements, which include digital identity, digital signatures, electronic payments, data sharing, digital post, and core government data registries, including open data initiatives**. He noted that the success of DPIs is contingent on trust between all actors, i.e., governments, the private sector, civil society, and citizens. **Undeniably, DPIs hold significant transformative potential, but their implementation requires careful, inclusive, and strategic planning that prioritizes trust, accountability, interoperability, transparency, national sovereignty, and inclusivity**. He also emphasised the importance of creating clear authorising and operational environments to better embed rule of law principles like legal certainty within DPI governance frameworks. Professor Watts underscored the importance of **shifting the discourse on DPI readiness and adoption beyond technical solutions to include legal, socio-political, and cultural considerations that often remain inadequately explored**. He urged experts in the workshop to deliberate upon **safeguards beyond legislative measures, such as institutional and social interventions, technical standards**, and more.

The workshop's primary objective was to deepen international discourse around trust and DPIs through candid reflection, dialogue, and shared learning across countries, as various jurisdictions explore the potential of DPIs to drive digital transformation for socio-economic inclusion. Through a critical approach, the workshop aimed not to dismiss the potential of DPIs, but to strengthen it. By interrogating gaps in existing systems, participants hoped to advance a more resilient and inclusive DPI ecosystem that truly serves public interest.

Participants at the workshop were representatives from various countries, including Australia, Brazil, the Democratic Republic of Congo, Germany, India, Jamaica, Japan, Kenya, Nepal, Nigeria, Peru, and the

United States of America. The discussion took place under Chatham House rules to encourage open and candid discussions.[2]

The workshop was structured around four focused group discussions (FGDs) covering the following themes:

1. **User Choice, Grievance Redressal, Accountability, and Safety**: To preserve user safety, accountability, and redressal mechanisms in DPI ecosystems;
2. **Data Privacy Concerns and Responsible Data Sharing**: To address challenges in data selection, collection, use, and governance in DPIs;
3. **Fair Private Sector Participation:** To examine how governance structures, market competition, and regulatory models shape the expansion of DPI ecosystems;
4. **Responsible Rollout and Equitable DPI Design**: To ensure that DPIs are designed and implemented equitably, prioritizing trust, transparency, dialogue, and inclusivity, particularly for marginalized communities.

Although the specific areas of focus differed for the four themes, the underlying structure of the discussion remained consistent: (a) identifying citizen or ecosystem-level limitations/challenges, (b) examining the effectiveness of existing regulatory and/or institutional safeguards, and (c) deliberating on future pathways for DPI preparedness that addresses the identified limitations.

Detailed observations from the thematic discussions are as follows.

Theme 1: User Choice, Grievance Redressal, Accountability, and Safety

Objective and Structure: Individual choice, safety, accountability, and redressal become important for DPI ecosystems, particularly in the face of **fraud, exclusion, and regulatory gaps**. In the backdrop of this context, the group began by interrogating the effectiveness of 'user choice' in digital welfare and service delivery, especially in digitally underconnected parts of the world. It identified limitations in data protection and public oversight safeguards that are exacerbated by fragmented accountability mechanisms due to the layered nature of DPI ecosystems with multiple service providers. The group concluded the discussion by providing future pathways for institutional and design-based approaches to advance security and accountability.

Summary of Key Insights:

- Rollouts of DPI systems in the Global South often **lack sufficient safeguards and turn populations into experimental grounds** for emerging and invasive technologies. Due to the absence of regulatory scrutiny, there is unchecked deployment of biometrics and data systems, without adequate safeguards for people's civil liberties.

[2] The Chatham House Rule helps create a trusted environment to understand and resolve complex problems. Its guiding spirit is: share the information you receive, but do not reveal the identity of who said it. Read more here: https://www.chathamhouse.org/about-us/chatham-house-rule

- **Data protection laws are either missing or filled with disproportionate exemptions for different actors**. This allows state and corporate actors to bypass safeguards through legal loopholes and further weaken citizen rights.
- **Publicly funded DPI systems operate with limited public oversight**, and therefore, citizens remain unaware of who collects their data, how it is shared, and the possible recourse when things go wrong.
- **Inclusion is undermined by weak infrastructure, low digital literacy, and a lack of service portability**. Offline access points are underdeveloped and are often unable to offer continuity across services or regions.
- **Financial DPIs face increasing threats of fraud,** which raises concerns about their status as critical infrastructure.

1. Designing for Inclusion in DPIs

The objectives and value systems of DPI funding and deployment initiatives require public debate that brings to light local governance realities. When funders carry out feasibility studies, it would be essential for them to not just incorporate the perspectives of governments and regulators, but also adequately incorporate local citizen and civil society perspectives, through inclusive consultations. This will help make DPI funding decisions more inclusive and citizen-centric.

Most existing data protection regimes are insufficient to regulate the use of DPIs and prevent their misuse. In case of existing data protection laws, some countries create blanket exemptions for state actors, or they fail to effectively regulate private sector data handlers involved in DPI ecosystems. As a result, the legal architecture does not meaningfully safeguard user rights or prevent institutional overreach. There is thus a need to embed use limitations, purpose limitation safeguards, and encourage the use of privacy-by-design principles to minimize risks of data misuse.

Fragmented accountability mechanisms for DPI – spread across state agencies, private partners, and platform owners – often make it difficult to determine who is responsible when systems fail. In the absence of clearly defined responsibilities across the DPI stack, not only does it become difficult to implement unified security protocols, but user complaints are also easily deflected or ignored. This ambiguity creates vulnerabilities that bad actors can exploit, leaving end-users exposed with a lack of clarity about who safeguards their interests. Additionally, reports[3] show that the National Payments Corporation of India's (NPCI) software that maps the Institutional Identification Number of an Indian NREGA[4] worker's bank linked with their national ID numbers ("Aadhaar") frequently runs errors and misdirects payments of these workers. **Experts highlighted that such errors are difficult to resolve at the local level because Aadhaar's supervisory authority, i.e., the Unique Identification Authority of India (UIDAI), has no dedicated grievance redress or social audit mechanisms for workers.** Since the Indian

[3] Narayanan, Rajendran. "The Efficiency Myth of Aadhaar Linking." The Hindu, December 29, 2021, sec. Comment. https://www.thehindu.com/opinion/op-ed/the-efficiency-myth-of-aadhaar-linking/article38067084.ece.

[4] India's National Rural Guarantee scheme that operates as a social welfare scheme that assists citizens fulfil their right to work, and offer livelihood security by earning a minimum wage for 100 days in a year.

Government made using Aadhaar-based Payment Systems mandatory[5] for wage payment to NREGA workers, several reports[6] of exclusion[7] and widening social insecurity have surfaced[8].

Digital inclusion efforts are misaligned with deeper access barriers. The digital divide is more than internet access—it is also about language, literacy, reliability of connectivity, and affordability. Currently, deployments of DPI often assume digital fluency and do not acknowledge structural exclusions that keep vast segments of the population from participating meaningfully in these systems.

Offline extensions of DPIs remain underdeveloped and poorly integrated. Despite examples of kiosks and local agent networks that enable access to DPI services in regions with low connectivity, these models are not always institutionalised at scale. Additionally, their lack of portability across regions or services limits their effectiveness, specifically for mobile populations or those who require continued access. While countries like India have introduced offline functionalities in UPI and Aadhaar (e.g., offline payments and verification), these efforts are limited by the **lack of portability in verification**. In India, Aadhaar can verify identity, but it does not **assure entitlement or access to benefits, such as food subsidies or access to electricity**. State and regional governments often have additional eligibility requirements for individuals to access social benefits. Furthermore, when individuals move across regions, they need to again adhere to the region-specific guidelines and reapply for benefits.

The mandatory adoption of DPIs for essential services risks entrenching digital exclusion. In situations where welfare schemes require digital authentication or DPI-based transactions, those unable to navigate the system, due to literacy, disability, or infrastructural gaps, are cut off from entitlements. This leads to a techno-solutionist approach[9] that prioritizes rollouts over readiness, and efficiency over equity.

2. Future Pathways

There is a need to enhance transparency and accountability in global DPI financing and governance, particularly in contexts with limited regulatory oversight. Incorporating independent social impact assessments and community-driven consultations will improve the design, funding, and deployment of DPIs. It will also help DPI deployments to remain responsive to local needs and uphold public trust.

---

[5] Internet Freedom Foundation. "No Place for Tech: How Digital Interventions in NREGA Are Undermining Rural Social Security," February 20, 2024. https://internetfreedom.in/no-place-for-tech-in-nrega/.

[6] Newsclick. "Aadhaar-Based Wages: 'Labelling 8.9Cr MGNREGA Workers "Ineligible" Shows Utter Disregard for Poor.'" January 4, 2024. https://www.newsclick.in/aadhaar-based-wages-labelling-89cr-mgnrega-workers-ineligible-shows-utter-disregard-poor.

[7] Buddha, Chakradhar, and Laavanya Tamang. "From Aadhaar Mandate to Mass Job Card Deletions | Economic and Political Weekly." The Economic and Political Weekly 58, no. No. 38 (September 23, 2023). https://www.epw.in/journal/2023/38/commentary/aadhaar-mandate-mass-job-card-deletions.html.

[8] NREGA Sangarsh (@NREGA_Sangharsh) "Basic statutory entitlements of right to work on demand & right to timely payment of wages is under threat. NSM strongly condemns this merciless regime's obsession with mixing technology & welfare, showing utter disregard for the poor, marginalised & working class. @MoRD_GoI", X, January 4, 2024, https://x.com/NREGA_Sangharsh/status/1742882924897395188.

[9] Techno-solutionism is a concept, originally defined by Evgeny Morozov, used to describe the belief that all complex social problems can be solved by technology. Morozov argues that this approach is often detrimental as it tends to overlook the social, political and ethical dimensions of a problem. Read Morozov interview on this concept here, Jiang, Kehan. "The Folly of Technological Solutionism: An Interview with Evgeny Morozov." Public Books (blog), September 9, 2013. https://www.publicbooks.org/the-folly-of-technological-solutionism-an-interview-with-evgeny-morozov/.

Governments must establish robust, rights-based data protection laws with narrow, clearly defined exemptions. Independent data protection authorities should be empowered to hold both state and private actors accountable. Moreover, **security in DPI must be broken down across different layers**—user interface, backend processing, data protection, and system-wide security.

Governments can draw on **lessons from legacy financial and public service infrastructures** with strong security and accountability. These practices can be adapted to digital infrastructures to ensure robust safeguards from the very beginning.

Outstanding Questions and Considerations for Informed Public Debate:

1. *How should grievance redressal mechanisms be structured to be effective across diverse DPI use cases?*
2. *How can safety and security frameworks be proactively embedded across DPI layers?*
3. *How do we extend DPI access to populations without digital connectivity, and how should verification systems be designed for offline functionality?*
4. *What mechanisms should be in place to prevent infringements of people's right to privacy and exploitative data practices, especially with governments being afforded broad exemptions under data protection laws?*
5. *How can external funding of DPI initiatives be better aligned with local needs and realities?*

Theme 2: Data Privacy Concerns and Responsible Data Sharing

Objective and Structure: This discussion focused on challenges in data selection, collection, processing, use, and general data governance for DPIs, exploring people's willingness to share data, and challenges with trust deficits and risks of exclusion. The group examined whether current safeguards—such as consent-based models and risk assessments—are sufficient and how data governance frameworks can be restructured to account for proportionality, context, and intended use.

It then critically assessed the limitations of the aforementioned safeguards while identifying the disproportionate burden placed on individuals in making privacy decisions. The group made the case for proportional data sharing, proposed a use-based data governance taxonomy, and evaluated the risks and potential of intermediary-based consent management models. The discussion concluded with reflections on the global shift away from consent-based regimes toward systemic safeguards and collective privacy approaches.

Key Insights:

- Erosion of citizen agency occurs when citizen participation in DPIs and the consequent sharing of personal data is effectively mandatory. This, combined with weak safeguards for data security, contributes to a trust deficit.

- Consent-based privacy frameworks place an unfair burden on individuals and are often ineffective in practice, especially in environments with low digital literacy and limited awareness of data risks.
- Structural safeguards, such as legitimate interest and accountability mechanisms, are needed to complement buyer-side protections like user consent to strengthen citizen agency and further foster trust.
- Data governance models should **classify data by intended use, not just by type**, to allow for **nuanced analysis of acceptable data use cases** in a context-driven manner.
- Trusted intermediary consent models like Account Aggregators **raise data maximisation concerns**, indicating the need for stronger oversight.

1. Trust, Compulsion, and Limits of Consent-Based Safeguards

Trust Deficit in DPI Systems: In the context of DPIs, **trust** is often cited as a foundational element in data sharing. However, its relevance diminishes when participation is effectively mandatory and users lack meaningful safeguards or user agency. For example, India's use of Aadhaar for accessing welfare benefits has shown how citizens are often compelled by on-ground actors (e.g., banks) to share biometric data despite the law providing for other options. Such practices normalize people feeling compelled to share their personal and often sensitive personal data, thus leaving data control and security as a secondary thought, at best.

While there was initial trust in DPI adoption due to convenience, **growing concerns about data breaches and misinformation have contributed to a trust deficit**. For example, in India, the personal information part of the Aadhaar database, including financial and demographic data, has been reportedly leaked[10] several times in the past. **In legally mandatory settings, trust can still be fostered through transparency, accountability, and strong protections for user rights.**

Exclusion Risks: The risks of exclusion also loom large. India's national ID-based social welfare programs have highlighted **exclusion concerns arising from the failure of tech-based solutions**. These can include technical authentication issues or small mismatches in the backend data stored within national ID databases. This challenge is accentuated for people from marginalized backgrounds. These exclusion risks underscore the need to build systems that prioritize equity, flexibility, and accessibility.

Inadequacies of Consent Frameworks: Current safeguards in DPI systems focus excessively on individual choice and buyer-side protections, such as opt-ins and informed consent. While consent is a significant safeguard, current systems require the user to process a lot of information, which is often complex, thus limiting the ability to make an informed individual choice and imposing a disproportionate burden on

[10] The Times of India. "Government, UIDAI Helpless as Instances of Aadhaar Misuse Reach Terrifying New Levels." Accessed May 23, 2025. https://timesofindia.indiatimes.com/readersblog/the-noose/government-uidai-helpless-as-instances-of-aadhaar-misuse-reach-terrifying-new-levels-9686/.

citizens[11]. Moreover, **consent-based frameworks are flawed** as individuals often struggle to comprehend the privacy implications of their choices.[12] While **risk assessment mechanisms** help organizations identify and reflect on possible risks, they rarely lead to meaningful system-level changes and safeguards in practice**.** There is thus an urgent need for structural safeguards on the supply side, such as recognising legitimate interest as a lawful basis for data processing, accompanied by robust accountability and risk assessment[13].

Emerging Global Concerns and the Role of Consent Intermediaries: Trusted intermediaries, i.e., third-party entities that manage data decisions on behalf of individuals, have been proposed as a solution to address user agency and data privacy concerns. **However, the potential for such intermediaries to turn into data monetization platforms that sell aggregated data for profit raises concerns about incentives.** Experts opined that it also does not seem to be an efficient solution for the inadequacies of the consent-based framework, and stakeholders argued that the model raises concerns of data maximisation. Thus, there is a need to explore solutions and frameworks that manage concerns of conflicting interests and ensure that consent is granted in privacy-first ways.

2. Towards Proportional, Use-Based, and Accountable Data Governance

The Need for Proportionality in Data Sharing: A fundamental principle that must guide future data governance frameworks is proportionality. Proportionality here refers to designing systems where data exposure is incremental, from anonymous to pseudonymous to fully identifiable, depending on the necessity of the use case. Unfortunately, many data-sharing frameworks do not account for proportionality, leading to excessive and unnecessary data collection.

Building a Taxonomy of Data Use: An additional shift is required in how data is classified and governed. **Data governance models should not only classify data by type (e.g., personal, sensitive, biometric) but also by intended use.** Such classification based on use case categories, such as public benefit use, private commercial use, individual-linked benefits, etc., will allow for a nuanced evaluation of acceptable versus unacceptable uses of data in a context-driven manner. This framework will help capture the **relational value of data** rather than viewing it in isolation.[14]

Successful Public Benefit Use Cases: Despite the contested role of intermediaries, there are examples of models that demonstrate how **aggregated data can be responsibly used for the public good**. One such

[11] "The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society." Centre for Information Policy Leadership and Bae, Kim & Lee, December 2024. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf.

[12] Flanagan, Anne Josephine, King, Jen, and Warren, Sheila. "Redesigning Data Privacy: Reimagining Notice & Consent for humantechnology interaction." World Economic Forum, July 2020. https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.

[13] "The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society." Centre for Information Policy Leadership and Bae, Kim & Lee, December 2024. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf.

[14] Soni, Shivam. "Fostering Participatory Data Stewardship | AAPTI Institute." Aapti Institute, June 7, 2023. https://aapti.in/fostering-participatory-data-stewardship/.

example is its use for urban mobility planning in Bengaluru, India[15]. However, these models become more complex when applied to sensitive data, such as healthcare records, as the stakes for privacy and consent are much higher.

The Shift Away from Consent-Based Models: The uneven digital literacy levels in many countries, including India, make it difficult for individuals to make informed consent and privacy decisions. In the US, representatives of the Federal Trade Commission (FTC) have expressed[16] reservations over the notice and choice model of consent. As global data governance conversations evolve, the focus is shifting towards protecting community interests. Policymakers and regulators globally are shifting away from surface-level fixes and are introducing human-centered design changes to make the consent process meaningful and ethical. For instance, the European Union General Data Protection Regulation (GDPR) includes design guidelines for notice and consent mechanisms, which also outlines prohibited types of interaction design such as pre-checked consent boxes and bundled consent.[17] Moreover, principles of privacy and security by design are increasingly being embedded into the technical architecture of DPI initiatives. This underscores the need to treat privacy as the default standard for any solution provider offering DPI-based products and services to citizens. A combination of regulatory frameworks and technical interventions is emerging as the way forward to achieve this balance.

In conclusion, a forward-looking DPI governance framework should incorporate proportionality, use-based classification, and systemic safeguards. Real and meaningful protections built into the design of digital systems will ensure that privacy is embedded in infrastructure, as opposed to it being contingent on digital literacy, user agency, or consent.

Outstanding Questions and Considerations for Informed Public Debate:

1. *What are systemic data protection and security safeguards that minimize user decision-making burdens?*
2. *How can data governance models adequately balance type-based and use-based approaches to regulation?*
3. *What safeguards are needed to ensure that data-sharing intermediaries act as trusted decision-makers?*
4. *How can data-sharing for public benefit (e.g., urban planning, healthcare) be balanced against privacy concerns?*
5. *How can an alternative or supplement to the consent-based framework be designed in a manner that does not place a disproportionate burden on the individual?*

---

[15] "Karnataka Open Data Initiative." https://karnataka.data.gov.in/.

[16] "The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society." Centre for Information Policy Leadership and Bae, Kim & Lee, December 2024. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf.

[17] Flanagan, Anne Josephine, King, Jen, and Warren, Sheila. "Redesigning Data Privacy: Reimagining Notice & Consent for humantechnology interaction." World Economic Forum, July 2020. https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.

Theme 3: Fair Private Sector Participation

Objective and Structure: This discussion explored the role of private sector participation in DPI initiatives, focusing on how governance structures, market competition, and regulatory models shape DPI ecosystems. The group began by interrogating the inconsistent and ambiguous use of the term 'open' and concerns of "open-washing". The group then examined the competing vision of state-led and market-driven approaches for DPI, and underscored the need to balance innovation, openness, and public interest while preventing monopolistic control and ensuring fair market conditions. The group concluded by discussing modalities for private sector participation such that it facilitates equitable and non-discriminatory access to DPI ecosystems.

Key Insights:

- Commercial incentives can shape DPI design in ways that may not align with public interest, making it crucial to assess the broader social impact of innovation pathways.
- The term "open" is often used inconsistently, leading to concerns of "open-washing"[18] and highlighting the need for clearer technical and governance standards.
- Protocol-driven systems (like India's Open Network for Digital Commerce) can lower entry barriers and foster interoperability, but they also present enforcement and accountability challenges across distributed actors.
- Regulatory capacity and state implementation systems remain uneven, raising questions about how to sequence DPI rollout and how (if at all) to proceed amid capacity deficits.
- There is a need for holistic governance frameworks that clearly define roles and responsibilities across state, private, and civil society actors to safeguard public interest.

1. Product Innovation Pathways and the Role of Open Models

DPIs have emerged as key enablers of innovation, with multiple models evolving to foster solution development within these ecosystems. Among these, the **'open protocol'** model provides a baseline digital infrastructure—usually state-led—upon which private actors can build innovative services. By contrast, the **'open market'** model sets common technical standards that allow multiple entities to interact seamlessly, reducing the risk of any one platform gaining undue dominance.

Undeniably, the participation of the private sector has been playing a crucial role in the deployment of DPIs. However, there can be mismatches between state-led visions for DPIs and market-driven approaches of private entities. Such mismatches can lead to outcomes that do not always serve the public interest. India's Open Network for Digital Commerce (ONDC) project, for instance, is a vision of the Indian government aimed at addressing the perceived competition challenges of traditional e-commerce

[18] The term "open-washing" refers to false claims by data publishers about the openness of their data while the data is really available under limiting terms. For more details, read Villum, Christian. "'Open-Washing' - The Difference between Opening Your Data and Simply Making Them Available." Open Knowledge Foundation blog, March 10, 2014. https://blog.okfn.org/2014/03/10/open-washing-the-difference-between-opening-your-data-and-simply-making-them-available/.

industries. However, several experts in India have pointed out that despite its open network design, there remain lingering issues of anti-competitive outcomes on ONDC.[19]

Compounding this is the **inconsistent use of the term "open"** in branding without clear technical or governance standards to back it up, thus contributing to **concerns of "open-washing".** While open-source is often associated with transparency and accessibility, that is not always the case. For instance, messaging applications like WhatsApp and Instagram Direct Messages (DMs) use the open-source Signal Protocol, but this does not imply that the entire service architecture is open-source or transparent.

Open-source projects may also need sustainable revenue models, including monetization through implementation, adaptation, support services, and upgrades. It is also crucial to **study the total impact of DPI initiatives to prevent unintended consequences, such as the exclusion of marginalized groups or the negative impact on people's civil and political rights**. Finally, defining what constitutes the "public" and "public interest" in digital governance lacks consensus. The significant involvement of private sector players in the development and deployment of DPI can also potentially create risks of dependencies in the hands of a few infrastructure and technical partners.[20] Thus, we need systems that hold these partners accountable, promote inclusive participation and minimise concerns of conflicts of interest and undue concentration of power. Open-source and open ecosystem initiatives should therefore factor these concerns at the governance, procedural and technical layers of DP projects.

2. Market Structures and Governance Challenges

The structuring of DPI markets requires deliberate regulatory design to prevent risks of monopolization, private control over public infrastructure, hollowing out of government capacity, and limited competition. In this context, the distinction between **protocol-driven models** and **quasi-regulatory institutions** becomes important. Protocol-based systems such as India's ONDC, built on the Beckn Protocol, illustrate a decentralized approach that promotes interoperability and unbundling. This can lower entry barriers for small retailers by enabling participation across different platforms. **Open protocols may function as regulatory mechanisms in themselves, but concerns remain over how they are governed and interpreted in practice.** A protocol-driven model can create competition but also presents challenges in enforcement, e.g., implementing a reliable[21] dispute resolution mechanism and pinpointing accountability[22] given the involvement of multiple network participants.

Stakeholders debated whether a **single market controller** is necessary or if **multiple governing entities** should oversee DPIs. For instance, the National Payments Corporation of India (NPCI), a non-profit entity

[19] M, Sarvesh. "Deep Dive: Will ONDC actually address competition concerns in e-commerce?." MediaNama, July 25, 2022. https://www.medianama.com/2022/07/223-ondc-competition-concerns-ecommerce-2/.
[20] Primus Partners and iSPIRIT. Beyond Boundaries: India's Digital Public Infrastructure (DPI) Model for Global Progress. https://primuspartners.in/docs/documents/Beyond%20Boundaries%20-%20India%E2%80%99s%20Digital%20Public%20Infrastructure%20(DPI)%20%20Model%20for%20Global%20Progress.pdf.
[21] Patodia, Susmit, Nitin Sharma, and Gokul Kumaravelu. "Unpacking the ONDC Opportunity: India's next Startup Catalyst." Accessed May 23, 2025. https://www.antler.co/blog/ondc-landscape.
[22] Panjiar, Tejasi, and Prateek Waghre. "Open Network for Digital Commerce (ONDC): An Explainer." Internet Freedom Foundation, March 10, 2023. https://internetfreedom.in/ondc-an-explainer/.

regulated by the Reserve Bank of India (RBI), acts as the sole governing body for UPI. While this centralized control has allowed for rapid adoption and standardization, concerns have been raised about the lack of competition, conflicts of interest, and alternative governance models.

In many emerging economies, **public procurement** remains a key driver of DPI infrastructure development, however, public investment remains sparse. While sustained investment is crucial for scaling and commercialization of DPI solutions, Global Majority countries must also proactively address procurement issues such as vendor lock-in and long-term dependency on single infrastructure providers. These efforts will preserve national sovereignty and ensure greater control over critical digital systems. Alongside this, **high entry barriers** limit competition—evidenced by the UPI ecosystem, where ~ 85%[23] transactions on the UPI network flow through only two service providers. These dynamics underscore the need to design DPIs that balance competition and control while safeguarding against monopolistic capture.

3. Regulatory and Technical Capacity Dilemmas

Since private participation in DPI initiatives seems extensive, the efficiency and sufficiency of regulatory mechanisms must keep pace through strong regulatory frameworks and institutional capacity to address issues of vendor lock-in or market concentration. While open-source and open standards can help mitigate vendor lock-in, they are not a silver bullet. Broader policy frameworks are required to preserve national sovereignty, ensure competition, facilitate fair procurement, and ensure fair market conditions. Here, **capacity constraints** — both in regulation and implementation—further complicate matters. Many governments lack the technical and administrative capacity to implement and govern DPIs effectively.

This raises a critical challenge: how to balance the advancement of DPI solutions with efforts to address capacity constraints. One approach may be to roll out DPI solutions through pilot phases or regulatory sandboxes, while simultaneously investing in strengthening **state and community capacity**. For instance, India's Common Service Centers (CSCs[24]), ASHA workers, women-led Self Help Groups (SHGs), and banking correspondents help enable widespread adoption of DPIs by providing digital and financial literacy at local levels[25]. Nonetheless, their role must be institutionally supported and strategically integrated. Additionally, governance playbooks developed for DPIs should outline responsibilities across all ecosystem players, including the state, private sector, and civil society.

Outstanding Questions and Considerations for Informed Public Debate:

1. *How can DPI governance balance protocol-driven models with the need for regulatory oversight to effectively guide market behavior?*
2. *How do we balance innovation and regulation without stifling competition or creating undue*

[23] Singh, Manish. "India Won't Enforce Payments Market Share Cap until 2025 in Win for Google and Walmart." TechCrunch (blog), December 2, 2022. https://techcrunch.com/2022/12/02/india-wont-enforce-market-share-cap-on-upi-until-2025-in-a-win-for-google-and-walmart/.
[24] "Achievements Made under Digital India Programme." Accessed May 23, 2025. https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=1885962.
[25] Tyagi, Dinesh. "How Digital Literacy Shapes Communities and Drives Sustainable Growth in India." Tech Observer (blog), November 5, 2024. https://techobserver.in/news/opinion/how-digital-literacy-shapes-communities-and-drives-sustainable-growth-in-india-288549/.

barriers? How can openness and interoperability be institutionalized to prevent vendor lock-in while allowing for sustainable business models?

3. *Can community-driven governance models provide an alternative to state-led regulation?*
4. *What safeguards are needed to ensure private sector participation aligns with public interest? What are the public accountability mechanisms for privately anchored DPIs?*
5. *How can capacity constraints be addressed in DPI rollout—can implementation and capacity-building proceed in parallel?*

Theme 4: Responsible Rollout and Equitable DPI Design

Objective and Structure: This discussion examined how DPIs can be designed and implemented equitably, ensuring trust, transparency, and inclusivity, particularly for marginalized communities. The group began the discussion by examining the role of various governance models for DPI implementation—whether state-led, public-private partnerships, or under non-profit control—in influencing citizens' trust levels towards DPIs. The group then explored how risks and trade-offs during DPI adoption differ for different social groups and how marginalized communities are often disproportionately affected. **The group finally underscored the importance of consultations and community participation before and during DPI rollout to strengthen citizen agency and to build on-ground trust**.

Key Insights:

- Proactive consultation tailored to specific community needs, before (and during) the DPI rollout, can help engender trust within on-ground and marginalised communities.
- Different governance structures and ownership models (state-led, PPPs, non-profits) impact public scrutiny and accountability.
- Different social groups may experience varying trade-offs and risks during DPI adoption.
- Challenges arise in tracking DPI development due to a lack of transparency, information asymmetry, and diminished civil society oversight/visibility.

1. Considerations for DPI Rollout and Adoption

Ownership Structures: As previously highlighted, the definition of DPI remains amorphous and complex. Thus, it becomes necessary to think about the ownership structures of the actors involved in the design and rollout of DPIs. Trust dynamics among the consumers/public are dependent on whether a government agency, a public-private partnership (PPP), or a private entity leads the DPI rollout and adoption.

Supervision of DPI implementation by a non-profit (instead of a State regulator) may result in efficient allocation of resources at scale. However, this may also result in a lack of accountability of these non-profit entities since they might be exempt from public scrutiny in a way that government/regulatory institutions are subject to transparency mandates under Freedom of Information (FOI) laws.

Conversely, the implementation of DPIs by the government can create other complexities. The presence of mistrust and disconnect between citizens and federal governments may directly impact the scale of adoption of the DPI. Low levels of trust may also arise from parallel shortcomings in baseline infrastructure, such as low internet penetration, which directly impacts access to DPIs.

Furthermore, while citizens may be able to hold the implementing government entity accountable through public scrutiny mechanisms, indiscriminate disclosures instead of accountability-oriented transparency may also create new risks, such as misuse of disclosed data by bad actors. Thus, it is a double-edged sword that must be balanced in a way that does not compromise the integrity of DPIs while also allowing public scrutiny.

Information Asymmetry: It is equally important to reflect on how meaningful the information accessed through FOI or Right to Information (RTI) laws is. Mere tracking of aggregate adoption numbers may not provide a comprehensive picture. Instead, access to information/data at a more disaggregated level can help assess exclusionary risks that may disproportionately affect marginalized communities. **Stakeholders argued that granular transparency can assist with targeted interventions and help improve the potential for inclusion through DPIs**.

Bias and Discrimination: Beyond the absolute numbers of adoption, it is also worth thinking about the relationship of different communities with technology and its associated benefits. For instance, in Brazil, Black women and other women of colour face different trade-offs in privacy vs. access to government benefits, as compared to other demographics.

Citizens' Agency: The adoption of DPI, which is otherwise voluntary on paper, is often mandatorily imposed on users, thus weakening their autonomy.

The Role of Geo-politics and DPIs' Potential for National Resilience: Some countries are exploring DPI as a mechanism to extend influence in other Global Majority countries. For instance, India's biometric digital ID initiative, Aadhaar, and digital payment interface, UPI, are being adopted and replicated globally. DPIs are also being used as a hedge against disproportionate dependence on foreign tech platforms.

Thoughtful identification of use case: In the backdrop of widespread and enthusiastic DPI rollout, it is worth reflecting on whether DPI is always the best solution for a country's challenges, or if its use should be more selective. Notably, the South Africa G20 Declaration[26] reflects some skepticism about whether DPI should be the default approach for all policy challenges. For example, Brazil is exploring DPI as a tool to address sustainability issues, while India's Ayushman Bharat Digital Mission (ABDM), which envisions a seamless digital health ecosystem, aims to improve healthcare access.[27] However, a deeper investigation

[26] G20 South Africa 2025. "Digital Economy," n.d. https://g20.org/track/digital-economy-2/.

[27] The Rural Environmental Registry (CAR) in Brazil is a tool that brings together data on rural properties and incorporates environmental information. This database allows for use in control, monitoring, environmental and economic planning and in combating deforestation. CAR is an example of government entities using these digital solutions to achieve the Sustainable Development Goals (SDGs). https://www.dataprivacybr.org/wp-content/uploads/2024/11/20241104-Relatorio-IPD-BPD-1.pdf

must be conducted to assess in what scenarios DPIs are solving on-ground challenges. This calls for strong processes through which DPI use cases are selected within any local context.

2. Pathways to a citizen-centric DPI rollout

Inclusive and Proactive Consultations: Establishing public trust in DPIs necessitates engagement well before implementation. This requires proactive consultations with communities, tailored to the specific jurisdiction and population. Proactive stakeholder interviews should be conducted using targeted questions that address key concerns related to governance, regulation, and rulemaking.

Bridging the Gap: There is a need to establish mechanisms that effectively communicate community perspectives, particularly those of marginalized groups such as the LGBT community, to government stakeholders. Mapping the diverse and heterogeneous viewpoints within the population is essential to ensure inclusive DPI development.

Including community perspectives through participation: Local governance structures, such as village chiefs and community organizations, can serve as vital intermediaries, facilitating DPI adoption at the grassroots level and communicating citizen feedback to the government.

Strengthening Accountability and Individual Choice: Central to citizen-centric DPI is the prioritization of individual choice. Governments can help people make informed choices by proactively disclosing project details, thereby enabling public assessment of safeguards.

Alleviating Sovereignty Risks: The adoption of open-source DPIs—when implemented in both letter and spirit—can help mitigate sovereignty risks. Such open-source DPIs enable governments to exercise local control while allowing for global interoperability.

Outstanding Questions and Considerations for Informed Public Debate:

1. *How can governments structure DPI adoption processes to build trust early on, rather than seeking trust after implementation?*
2. *How should one choose the most appropriate governance model for DPI implementation—whether state-led, through public-private partnerships, or under non-profit control?*
3. *How can DPIs ensure the representation of marginalized groups in governance structures and prevent exclusionary design?*
4. *How should transparency in DPI projects be managed to balance accountability with security risks?*
5. *How can governments work with citizens to identify sectoral use-cases that genuinely merit DPI pilots, and ensure those pilots prioritize citizen rights and public interest from the outset?*

Findings and Next Steps

Learning and Unlearning: The rapid growth and hype surrounding digital development initiatives, specifically DPIs, must not distract from the necessity of centering local community needs in DPI design, rollout, and adoption. The attractiveness of digitally-mediated welfare and service delivery solutions must not overshadow the on-ground realities of exclusion risks and deprivation of agency, especially for marginalized communities that they were primarily meant to serve.

Discussions on governance structures highlighted that robust accountability measures for all stakeholders are critical to balance innovation with public interest. It is of utmost importance to unlearn that the consent framework of data protection is, by itself, a sufficient measure of empowering citizens to make an informed and meaningful choice. It is equally necessary to learn that vulnerable social groups are often disproportionately affected by risks of non-inclusive and non-representative DPIs.

Although institutional, legal, and social safeguards exist for mitigating the above-identified risks and limitations, they may not always achieve the intended outcomes, especially if the conception and implementation process lacks proactive and sustained engagement with diverse communities. **The deliberations during the workshop raised actionable insights as well as open questions, both crucial to informing public debates on DPI preparedness and risk mitigation.**

Acknowledgements

Authors:

- Tejasi Panjiar
- Dr. Sohini Dutta

Research Supervised and Edited By:

- Namrata Maheshwari
- Alison Howe
- Max Heinrich
- Rohit Kumar
- Sidharth Deb

We would like to thank all the workshop participants for sharing their expertise and invaluable insights. All errors and omissions remain the sole responsibility of the authors.

Citation Recommendation

Panjiar, Tejasi, and Dutta, Sohini. “From Risk to Resilience: A Rights-based Approach to Digital Public Infrastructure (DPI) Readiness in the Global Majority.” The Quantum Hub, July 16, 2024.

July 2025

www.thequantumhub.com

The Quantum Hub (TQH)
No. 29-30, Lala Lajpat Rai Marg, Lajpat Nagar III
Delhi - 110024 +91-11-4084-5940

office@thequantumhub.com