**Artha Global's comments on the Universal DPI Safeguards Framework**

*November 2024*


**1. Overall Feedback** ..... **2**

*1.1. The need for a unique approach to safeguards for DPI* ..... *2*

*1.2. Linkages to ecosystem efforts and literature on safety and inclusion* ..... *3*

*1.3. Stakeholder understanding of digital transformation and DPI* ..... *4*

**2. Specific Feedback** ..... **5**

*2.1. Risks to Safety* ..... *5*

2.1.1. Privacy vulnerability ..... 5

2.1.2. Digital insecurity ..... 6

2.1.3. Physical insecurity ..... 7

*2.2 Risks to Inclusion* ..... *8*

2.2.1 Discrimination ..... 8

*2.3 Structural vulnerabilities* ..... *9*

2.3.1. Digital distrust ..... 10

2.3.2 Weak rule of law ..... 11

2.3.3. Weak institutions ..... 12

2.3.4. Technical shortcomings ..... 13

*2.4. When? The Iterative DPI Life Cycle* ..... *13*

2.4.1. Development ..... 13

*2.5 Adopting the Framework* ..... *14*

2.5.1. Building Capacity ..... 14

## 1. *Overall Feedback*

The United Nations Universal Digital Public Infrastructure (DPI) Safeguards Framework (hereafter, "the Framework") and the accompanying 'Guide to Building Safe and Inclusive DPI for Societies' (hereafter, "the Report") represent a significant step in the global effort toward DPI-led digital transformation. With rising interest and investment in DPI globally, the role of the Universal DPI Safeguards Initiative in elevating the need for safeguards and inclusion is timely and addresses an urgent need. The Report provides critical and currently absent foundations to the DPI ecosystem by way of a common vocabulary—such as the DPI lifecycle, key DPI implementation stakeholders (referred to as responsible authorities), risks, and guiding principles. Furthermore, the Report grounds this discussion within a human rights framework, emphasising safety and inclusion as core attributes for DPI initiatives, and DPI's role as a means to achieving development goals. The Report outlines the approach to the Safeguards framework, with the objective of equipping practitioners with practical mitigation strategies linked to identified risks, making it a valuable and actionable tool for individuals and organisations working on effective DPI implementations for safe and inclusive societies.

We appreciate the opportunity to contribute our perspectives to the Report. Drawing on our past work and in-depth experience in the DPI ecosystem, our review is aimed at sharpening the theory of change articulated in the Report. The first part of this review presents our broad recommendations, and the second part offers targeted suggestions for specific parts of the Report. Our review is restricted to the Report, and does not cover the contents of the Process and Practice recommendations in Framework v1.0.

### 1.1. *The need for a unique approach to safeguards for DPI*

The Report states that the Framework is based on five "dimensions"—stages of the DPI lifecycle, the responsible authorities involved throughout that lifecycle, risks to be mitigated, principles to be upheld in DPI design and implementation, and recommendations to translate principles to action. While these dimensions are undoubtedly important in the context of any technology aimed at delivering public or private services, the Report does not sufficiently explain why this particular Framework is needed. It describes the Framework as "approach and definition agnostic," implying it can be applied to any large-scale technology, such as identity systems, social protection systems, access to justice, and health workflows. However, this raises an important question: how does this Framework differ from other design or implementation frameworks already developed for these systems?

For example, the World Bank's practitioner's guide for digital ID implementation under the ID4D project also addresses similar risks, principles, and planning roadmaps.[1] Likewise, the World Bank's Social Registries for Social Assistance and Beyond: A Guidance Note &

[1] World Bank. (n.d.). SECTION II. Designing an ID system | Identification for Development. https://id4d.worldbank.org/guide/section-ii-designing-id-system

Assessment Tool[2] provides a comprehensive resource for implementing safe and inclusive social registries. Given the availability of such resources for individual DPI, the need for the DPI safeguards framework needs to be articulated.

This can be addressed by articulating why existing frameworks for digital transformation and e-government are insufficient or inadequate when applied to DPI. The Report should explicitly outline why this unique approach to safeguards is necessary. Conversely, the Report can explain how the framework borrows and learns from existing knowledge, and its applicability to digital transformation work globally.

In addition, the Report understates a critical aspect of DPI that distinguishes them from other technological solutions—their broader public, common, and infrastructural value.[3] DPI are more than just large-scale technological systems; they enable the creation of new services and interactions across citizens, governments, and businesses, transforming the digital economy. While the Report acknowledges the risks associated with digitalisation, it does not sufficiently focus on the unique capabilities of DPI to operate at scale and drive innovation.

This gap in the Report highlights a broader issue: it attempts to propose a framework for implementing DPI without clearly defining what makes DPI unique or how they differ from earlier digital transformation efforts. To be effective, the Framework must build on this distinction, emphasising the unique infrastructural and transformative capabilities of DPI and explaining why they require a distinct set of safeguards.

### *1.2. Linkages to ecosystem efforts and literature on safety and inclusion*

The Report states that the "DPI Safeguards Initiative is grounded in principles enshrined in the Universal Declaration of Human Rights (UDHR), which serves as the foundation for international human rights law, including treaties such as the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights." The Framework is also guided by the Sustainable Development Goals (SDGs) and the UN Secretary-General's Roadmap for Digital Cooperation.

While aligning with the UDHR indicates that the Framework's five dimensions aim to protect and promote human rights in relation to DPI, and the SDGs and the Roadmap emphasise the need to mitigate harms from deploying technologies for development, this alignment alone is insufficient. The Framework and its dimensions should also derive legitimacy from the well-researched field of digital transformation. The lack of references to relevant literature that supports these DPI-specific dimensions is a significant shortcoming. Although the Report includes a "non-exhaustive list of knowledge resources relevant to the framework" in the

---

[2] Leite, P., George, T., Sun, C., Jones, T., & Lindert, K. (2017). Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment tool.
https://documents1.worldbank.org/curated/ar/698441502095248081/pdf/117971-REVISED-PUBLIC-Discussion-paper-1704.pdf

[3] Eaves, D., Mazzucato, M., & Vasconcellos, B. (2024, May 28). *Digital public infrastructure and public value: What is 'public.'* UCL Institute for Innovation and Public Purpose.
https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi

appendix, it fails to explain how these resources were interpreted or used to define the chosen dimensions. This absence of citations and referencing within the main text weakens the rationale for the Framework, and its valuable contributions, such as the principles, responsible authorities, and the DPI lifecycle. Furthermore, the knowledge resources included in the appendix are all from multilateral organisations or convenings, particularly from the global north. A significant amount of work has been done by civil society organisations around the world, particularly in the global south where DPI are mostly deployed, which are worthy of inclusion.

The Report can remedy this by providing insight into the Initiative's learnings from the stakeholder engagement process. Providing details on how the engagements were conducted, who was consulted, what perspectives were gathered, and how they informed the dimensions would add much-needed transparency and confer greater legitimacy to the Framework and its dimensions. This would also strengthen its value as a 'unified approach to safeguards' and a platform to bring together efforts by civil society organisations, development partners, the private sector and governments.

### *1.3. Stakeholder understanding of digital transformation and DPI*

The Report assumes that stakeholders have prior knowledge and a strong understanding of the many dimensions of the domain of digital transformation. This assumption is evident in how the Report presents its arguments and articulates key points.

For example, the Report identifies privacy vulnerability as a risk to user safety, defining it as occurring when "personal information is processed (shared, stored, or used) without consent, beyond reasonable privacy expectations, or misused to cause harm." However, this definition assumes that stakeholders understand how such privacy risks manifest within the context of DPI or can make the connection between privacy violations and DPI risks (see subsection 2.1.1 for more details).

Similarly, the Report introduces the concept of structural vulnerabilities, defined as "vulnerabilities that exist at the systemic level" that "limit the effectiveness of safeguards." It lists five such vulnerabilities: weak rule of law, weak institutions, digital distrust, technical shortcomings, and unsustainability. However, the Report does not clearly explain these terms, leaving readers to assume that they refer to societal, political, and legal weaknesses that undermine the safeguards. Moreover, it presumes that stakeholders already understand how these vulnerabilities can obstruct the successful implementation of the proposed safeguards (see subsection 2.1.1. for more details).

Overall, the Report relies heavily on the assumption that stakeholders have prior expertise in these areas, making it difficult for those without such background knowledge to fully grasp the risks and challenges it outlines.

## 2. *Specific Feedback*

To strengthen the articulation of the risks, structural vulnerabilities, and adoption considerations for the Framework, the sections below have specific and detailed feedback, with suggested resources.

### *2.1. Risks to Safety*

#### *2.1.1. Privacy vulnerability*

The Report discusses the risk of privacy vulnerability, assuming stakeholders are already familiar with the privacy violations and data protection challenges that can arise in DPI. It states that privacy violations occur when personal information is processed without consent, "beyond reasonable privacy expectations or misused to cause harm." However, this explanation assumes stakeholders:

- Understand reasonable privacy expectations in the DPI context: The Report does not explain privacy expectations in the DPI context. Since DPI systems typically collect and process large volumes of data, the government managing and building these digital systems is a threat to individual privacy.[4] Moreover, privacy safeguards required for digital IDs or a data exchange platform may differ from those needed for a digital payment platform and reasonable privacy expectations may also vary across jurisdictions, shaped by each society's socio-political and cultural understanding of privacy.

- Are familiar with the taxonomy of harms caused by data misuse: While the Report references Solove's taxonomy of privacy harms[5]—such as physical, financial, psychological, emotional, and reputational—it does not explain what these harms mean or demonstrate how they manifest in specific DPI contexts that undermine safety. For instance, it would be helpful to illustrate how financial or reputational harm might result from a data breach in a social registry or digital ID database. Although the consequences of a data breach are not always immediately apparent, the U.S. government's response to the Equifax data breach offers a useful example. The breach exposed the sensitive information of 150 million Americans. As part of a settlement, Equifax was required to provide affected individuals with free credit monitoring or a cash payment of $125.[6] Additionally, customers could request compensation of up to $20,000 and receive six free credit reports annually.[7] This settlement ensured that individuals were compensated for any potential financial losses resulting from the breach.

---

[4] Sherman, J. (2024). *Finding security in digital public infrastructure*. The Atlantic Council. https://www.atlanticcouncil.org/uncategorized/finding-security-in-digital-public-infrastructure/
[5] *A Taxonomy of Privacy - ORG Wiki*. (n.d.). https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy
[6] Epic.org. (n.d.). *Equifax Data Breach*. Epic.org Electronic Privacy Information Centre Web Site. https://archive.epic.org/privacy/data-breach/equifax/
[7] Ibid

Furthermore, the Report focuses only on harms arising from the processing of personal information without consent, overlooking the complexities of relying on consent as a primary safeguard, especially for marginalised individuals. Research indicates that individuals often do not fully understand what they are consenting to. In many countries, DPI like digital ID and social registries are legally required to access welfare benefits, leaving individuals with no realistic choice but to consent to processing of their personal information. These individuals often lack clarity on how their data will be used or for what purpose. Even when privacy notices are provided, they are often written in a way that fails to meaningfully inform individuals of potential harms or available recourse mechanisms. This reveals a critical flaw in the consent-based approach to privacy protection. Therefore, we recommend reconsidering this approach when advocating for privacy safeguards within DPI as consent should not preclude businesses and governments from accountability due to privacy harms. Data collectors—whether businesses or the state—should be held accountable for any privacy harms caused to individuals or groups, regardless of whether consent was obtained.[8]

*2.1.2. Digital insecurity*

The Report discusses the risk of digital insecurity in a way that does not appropriately capture its threat in the following ways:

- Inadequate articulation of the severity of digital insecurity: The description in the section falls short of explaining why digital insecurity "extends beyond" privacy vulnerabilities. The Report discusses digital insecurity from a systemic perspective, emphasising that safe and secure systems are critical because they form part of an essential digital infrastructure. Through this, we understand that digital insecurity risks include both privacy risks and broader systemic risks, with repercussions of these risks overlapping, but in different contexts. For instance, system wide data breaches may not be targeted to individuals, but instead, may undermine data stored across nations. The WannaCry ransomware attack that took place in 2017, exploited vulnerabilities in outdated software across 156 nations and multiple sectors.[9] The National Health Service in the U.K. was particularly impacted with disruptions in ambulance handover processes and patient data systems. The attack was not targeted at individuals but to the broader infrastructure, demonstrating how a system-wide breach can undermine national data and affect entire sectors, potentially leading to widespread physical and reputational harm across a nation. This distinction is important and should be made explicit to effectively convey the severity of digital insecurity.

- Assumption of prior knowledge: The section does not cite literature to support its arguments; this creates ambiguity and weakens its ability to precisely convey the consequences of digital insecurity. For instance, in the sentence, "Digital insecurity extends beyond privacy vulnerabilities, encompassing service outages and sector-wide disruptions and **other forms of systemic instability**," the phrase in bold is too broad and

[8] Matthan, R. (2024, October 9). *Homo privaticus*. Ex Machina. https://exmachina.in/09/10/2024/homo-privaticus/

[9] NHS England. (21 April, 2023). NHS England business continuity management toolkit case study: WannaCry attack. https://www.england.nhs.uk/long-read/case-study-wannacry-attack/

ill-defined. Similarly, in the sentence, "Inadequately secured systems are susceptible to exploitation for malicious purposes, including . . . the **destabilisation of nations,**" the phrase in bold lacks clarity. In the first example, the Report assumes that stakeholders are familiar with the types of systemic instability being referred to. In the second example, it assumes that stakeholders understand how and why an inadequately secured system could contribute to the destabilisation of nations. These phrases prevent stakeholders from fully understanding the scope and implications of digital insecurity. To improve clarity, the Report should define these terms more precisely through supporting resources.

*2.1.3. Physical insecurity*

The Report discusses physical insecurity in a way that does not sufficiently explain what it is and why it is particularly relevant. To improve clarity, we recommend:

- Distinguishing physical insecurity from physical harm: The Report states that physical insecurity arises from digital insecurity, however, it does not sufficiently explain how this differs from "physical harm," a risk that arises from privacy violations. We understand physical harm as a risk that may have individual repercussions which can lead to bodily injury or death.[10] For instance, the case of Rebecca Schaeffer, a model and actress, who was murdered after a stalker obtained her home address with the help of a private investigator is an example of the individual repercussions of a physical harm.[11] On the other hand, we understand physical insecurity in the context of groups that may not have immediate and personal repercussions to individuals. [Since the the Report explains that "physical insecurity often stems from digital insecurity."] For instance, during Hong Kong's pro-democracy protests between 2019-2020, law enforcement authorities used facial recognition technology to target protesters.[12] Through databases of personally identifiable information, protesters sharing similar political opinions were targeted as a whole, affecting the physical safety of this group. This distinction between physical harm at an individual level and physical insecurity at a system-wide level that may have widespread consequences for groups with shared vulnerabilities should be clarified.

- Explaining why physical insecurity is prioritised over other types of harm: The Report should elucidate why physical insecurity is emphasised over other types of system wide harms, such as financial, reputational, or psychological insecurity. The consequences of which may be similar in magnitude to those that arise from physical insecurity. For instance, the 2014 JP Morgan Chase hacking compromised the accounts of 76 million

[10] Citron, D., & Solove, D. (2022). *Privacy Harms*. BU Law Review. https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf
[11] Weisholtz, D., & Caulfield, P. (2019). *Why actress Rebecca Schaeffer's 1989 murder was Hollywood's wake-up call*. Today. https://www.today.com/news/why-actress-rebecca-schaeffer-s-1989-murder-was-hollywood-s-t157444
[12] Mozur, P. (2019). *In Hong Kong Protests, Faces Become Weapons*. The New York Times. https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html

households and seven million small businesses. Sensitive information about the names, addresses, phone numbers and emails of these users exposed them to risk of physical and psychological harm.[13] Doxing—the disclosure of personal data to facilitate people being located, contacted, and harassed—involves two types of harms. A risk of physical harm as well as psychological harm consisting of the fear that accompanies the risk of physical harm.[14] Privacy harms that arose from the JP Morgan Chase hacking were multifaceted and may have consisted of harms beyond potential physical harm. If the Report considered such paradigms but still determined that physical insecurity was the most significant, providing a rationale for the choice would greatly benefit stakeholders.

*2.2 Risks to Inclusion*

The Report acknowledges that discrimination, unequal access, and disempowerment are forms of exclusion which undermine inclusivity and accessibility. However, the current representation in the Report suggests that discrimination, unequal access, exclusion, and disempowerment operate at the same level of risks to inclusion. Exclusion is the primary risk to inclusion and it can be the outcome of discrimination, unequal access, and disempowerment. This distinction needs to be clearly articulated and appropriately visually represented.

*2.2.1 Discrimination*

As a unified safeguards Framework for **all** DPI, to ensure consistency throughout the Report, we recommend highlighting:

- Discrimination in other DPI systems: The Report states that "it is **particularly important** to avoid discrimination in digital ID systems that provide social and emergency services, government services, and enable the broader economy." In doing this, it suggests that the risk of discrimination is especially pronounced in digital ID systems. While the all-pervasive nature of DPI-based ID systems and the risks that arise are well-known, it is key to ensure that the risks (and consequently mitigations) adequately focus on discrimination in other DPI. For instance, the South African Social Security Agency, which administered social security grants awarded Cash Paymaster Services (CPS) an exclusive contract to deliver social security benefits in 2012. As the country grew dependent on this monopolist, companies exploited CPS' 'customer base' to cross-sell services including life insurance, mobile money, and loans. Payments for these services automatically deducted from beneficiaries' social security grants, making it especially easy to enrol. However, the widespread access to this customer base and grant money allowed these companies to defraud millions of South Africans. Recipients of the social security grant, a critical government benefit, did not always

[13] Rushe, D. (2014). *JP Morgan Chase reveals massive data breach affecting 76m households*. The Guardian. https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach

[14] Citron, D., & Solove, D. (2022). *Privacy Harms*. BU Law Review. https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf

receive their full due amount.[15] In this instance, a digital payment system was central to providing essential state benefits, and it is just as important to avoid discrimination in these systems. Thus, the Report should highlight the importance of all such DPI systems, with no particular focus on ID systems.

- Discrimination as a consequence of interoperability: DPI are envisioned to be interoperable for seamless exchange of information across digital systems.[16] This interoperability can lead to discrimination in one system cascading to other connected systems. For instance, in 2016, Robodebt was introduced in Australia; this system relied significantly on automation and used Australian Tax Office data and income-averages to estimate welfare recipients' debts to the Commonwealth Government agency.[17] Between 2016 and 2019, the Robodebt scheme raised more than half a million inaccurate debts.[18] Subsequently, the Australian Government paid more than $751 million in unlawfully claimed debts and $112 million in compensation to approximately 400,000 people.[19] This level of harm was enabled through automation and the interlinking of multiple digital systems. The distinction between discrimination in siloed digital systems and systems that enable interoperability should be made explicit in the Report to appropriately highlight the unique consequences of discrimination due to interoperable DPI systems.

*2.3 Structural vulnerabilities*

The Report identifies five structural vulnerabilities [digital distrust, weak rule of law, weak institutions, technical shortcomings, and unsustainability]. From these, we understand that the diverse operating environments in countries—cultural, political, social, economic— are not only risks to DPI implementations but may also weaken the effective implementation of safeguards. This is an essential consideration for any DPI implementation framework.

The Report does not clearly define these vulnerabilities and stakeholders are left to assume that they refer to societal and political weaknesses that hinder the effectiveness of reforms, including DPI. While the Report highlights the potential effects or outcomes of these vulnerabilities, it does not state what they are, or explain its implications for the effectiveness of the Framework.

---

[15] Center for Human Rights Global Justice. (2021). Locked In! How the South African Welfare State Came to Rely on a Digital Monopolist. https://chrgj.org/2021-03-11-locked-in-south-africa-welfare-state-digital-monopoly/

[16] Massally, K., Matthan, R., & Chaudhuri, R. (2023). *What is the DPI Approach?* Carnegie India. https://carnegieendowment.org/research/2023/05/what-is-the-dpi-approach?lang=en

[17] Karp, P. (2019). *'Pay the money back': robodebt, the Coalition's backflip and how it 'hounded' welfare recipients.* The Guardian. https://www.theguardian.com/australia-news/2019/nov/22/pay-the-money-back-robodebt-the-coalitions-backflip-and-how-it-hounded-welfare-recipients

[18] Victoria Legal Aid. (n.d.) *Learning from the failures of Robodebt – building a fairer, client-centred social security system.* https://www.legalaid.vic.gov.au/learning-from-the-failures-of-robodebt

[19] Victoria Legal Aid. (n.d.) *Learning from the failures of Robodebt – building a fairer, client-centred social security system.* https://www.legalaid.vic.gov.au/learning-from-the-failures-of-robodebt

*2.3.1. Digital distrust*

The Report's explanation of digital distrust does not fully capture how it undermines the safeguards. To address this, we recommend the following:

- Use of descriptive language: The section uses vague language that weakens its ability to precisely convey the factors that contribute to and the consequences of digital distrust. For instance, in the sentence, "Like discrimination, distrust in DPI is often tied to **pre-existing social factors** that must be **acknowledged and understood** to be effectively addressed," the phrases in bold are too broad and ill-defined. The first phrase assumes familiarity with the pre-existing social factors that may contribute to digital distrust. To improve clarity, the Report should outline examples of such factors. For instance, low utility of the platform, low digital and financial confidence, low provider and agent integrity and competence, lack of grievance redressal mechanisms, and poor community perception are factors that may contribute to digital distrust in a population.[20] Similarly, in the second phrase, to "acknowledge and understand" pre-existing social factors, the Report should outline ways to address digital distrust, which may include facilitating user control over their data and ensuring data is exchanged in a manner that upholds user privacy and follows data security practices.[21] The lack of specificity prevents an appropriate explanation on how digital distrust may undermine the safeguards; addressing this may strengthen the Framework.

- Explaining digital distrust in the DPI context: While the Report acknowledges that digital distrust may present "serious risks to the legitimacy, effectiveness, adoption, and implementation of DPI systems," it does not appropriately highlight the importance of this in the DPI context. During the COVID-19 pandemic, the Indian government promoted the use of the 'Aarogya Setu' app to enable contact tracing and curb the spread of the virus. Many Indians, however, expressed concern over the app's effectiveness, risk of potential surveillance with the data collected, and fear of denied access to services.[22] Low levels of trust in the government's ability to collect, store, process, and use data curbed adoption, which may have delayed efforts to monitor the spread of the virus through contact tracing. Since DPI may facilitate the provision of benefits to populations at scale, lack of trust in institutions that provide these may hinder government efforts. Thus, the consequences of digital distrust in the DPI context should be effectively articulated.

- Incorporate all factors that may contribute to digital distrust: Safety and inclusion is the lens through which the Framework is developed but digital distrust is an outcome of a complex interplay of factors that may fall outside the purview of safety and inclusion.

[20] Kulkarni, A., Ashraf, H., & Ghosh, I. (2024). *Part 2: Is Lack of Trust Keeping Customers Away From Digital Financial Services? – Understanding the contours of trust.* Dvara Research. https://dvararesearch.com/is-lack-of-trust-keeping-customers-away-from-digital-financial-services-understanding-the-contours-of-trust-part-2/

[21] Bhattacharya, P. (2024). *Growing a digital trust ecosystem around DPI.* Express computer. https://www.expresscomputer.in/guest-blogs/growing-a-digital-trust-ecosystem-around-dpi/113639/

[22] Shashidhar, K. (2020). *Aarogya Setu App and its many conflicts.* Observer Research Foundation. https://www.orfonline.org/expert-speak/aarogya-setu-app-many-conflicts-67442

Speeds of transaction and payment delays when using digital payment services may breed distrust and curb widespread adoption. For example, instances of payment failures where the payment is deducted from the consumer's account but not from the merchant's account can be particularly stressful for low-income consumers, preventing them from using digital services.[23] This factor is outside the purview of safety and inclusion but is still a determinant of trust. We recommend either acknowledging other factors that may contribute to distrust, or presenting a rationale for how all factors fall under the umbrella of safety and inclusion.

*2.3.2 Weak rule of law*

The Report's explanation of the weak rule of law has two main issues:

- Assumption of prior knowledge: The section on weak rule of law assumes that the stakeholder understands how DPI enhances the power of those in control as seen in the sentence, "**As DPI can amplify the political, social, and economic power of those who control these systems**". To address this, the Report should explicitly detail how the deployment of DPI can individually affect political, social, and economic power.

  For instance, government surveillance in Turkey under President Recep Tayyip Erdoğan's administration has eroded civil liberties while increasing the government's political power.[24] Second, since DPI facilitates access to essential services, these systems may extend resources to previously underserved populations, thereby increasing the social power of entities that control DPI.[25] Third, DPI can drive economic growth by enabling faster transactions and lowering costs associated with traditional banking systems, as seen with Brazil's Pix payment system.[26] The introduction of more efficient financial processes has boosted economic power for the government.

  Explanation of the factors that may contribute to power should be made explicit to avoid assumptions about the stakeholder's prior knowledge. This may also better inform how concentrated power may undermine conventional institutions responsible for upholding the rule of law.

- Missing the contextualisation of the weak rule of law in DPI: While the Report outlines how power concentration may inhibit innovation and limit services, it does not appropriately contextualise the weak rule of law and its risk in DPI. Systems which

[23] Kumar, R., & Verma, M. (2017). *Addressing the barriers to adoption in digital payments*. The quantum hub. https://thequantumhub.com/wp-content/uploads/2020/08/Addressing-the-barriers-to-adoption-in-digital-payments-TQH-Consulting-Aug2017-Final.pdf

[24] Human Rights Watch. (2016). *Silencing Turkey's MediaThe Government's Deepening Assault on Critical Journalism*. https://www.hrw.org/report/2016/12/15/silencing-turkeys-media/governments-deepening-assault-critical-journalism

[25] Mohanty, A. (2023). *The Business Case for DPI*. Carnegie India. https://carnegieendowment.org/posts/2023/06/the-business-case-for-dpi?lang=en

[26] Chandra, et al. (2024). *From Brasilia to Bombay: The Unlikely Twins Leading a Global Open Finance Revolution*. Centre for Digital Public Infrastructure. https://cdpi.dev/wp-content/uploads/2024/09/DPI-for-Open-Finance-A-case-study-on-UPI-Pix-1.pdf

collect and store large amounts of personally identifiable data may be used as tools of monitoring and surveillance.[27] For instance, the collapse of the Islamic Republic of Afghanistan under President Ashraf Ghani and the reinstatement of the Islamic Emirate of Afghanistan under the Taliban allowed the Taliban to access American devices that store biometric information of Afghan citizens.[28] This has since enabled the Taliban to crack down on political opponents and dissenters, with one of the most brutal attacks being when Taliban soldiers stopped a bus in Afghanistan's Kunduz province and conducted biometric scans of the passengers, and those identified as part of the Afghan National Defence Force were targeted and killed.[29] The consequences of DPI implementation in a country with a weak rule of law is important and should be made explicit to convey the severity of risk.

*2.3.3. Weak institutions*

The Report's explanation of weak institutions lacks specificity which does not allow it to effectively capture how weak institutions may undermine DPI safeguards. To address this, we recommend strengthening instances of:

- Vague use of language: When describing the "necessary policies and practices" that are important to implement to bolster the effectiveness and legitimacy of safeguards, the Report should highlight how a lack of robust legal protections for personal data can exacerbate fears regarding privacy and undermine safety,[30] or how a lack of transparency and accountability could breed distrust, hinder adoption, and subsequently undermine the safeguards.[31] We recommend providing examples of such policies and practices which may be integral to uphold the effectiveness and legitimacy of safeguards.

*2.3.4. Technical shortcomings*

The Report discusses technical shortcomings that include risks which may arise from "inappropriate technology choices." However, these types of sub-optimal choices are a consequence of a "strategic and governance shortcoming" rather than a technical shortcoming. If the Report defines "technical" differently, it should be appropriately explained.

---

[27] Agote, A. (2023). *India's DPI Success: A Global Blueprint.* IE Insights. https://www.ie.edu/insights/articles/indias-dpi-success-a-global-blueprint/

[28] Jacobsen, K. (2022). *Biometric data flows and unintended consequences of counterterrorism.* International Review of the Red Cross. https://international-review.icrc.org/articles/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916

[29] Privacy International. (2021). *Afghanistan: What Now After Two Decades of Building Data-Intensive Systems?* https://privacyinternational.org/news-analysis/4615/afghanistan-what-now-after-two-decades-building-data-intensive-systems

[30] Sur, A. (2024). *MeitY raises alarm over data breaches impacting trust in DPI initiatives.* Money Control. https://www.moneycontrol.com/technology/meity-raises-alarm-over-data-breaches-impacting-trust-in-dpi-initiatives-article-12785484.html

[31] Gaur, R., & Diamond, A. (2024). *Digital public infrastructure can bring enormous benefits – or pose significant risks. Safeguards make the difference.* Digital Impact alliance. https://dial.global/dpi-can-bring-benefits-or-risks-safeguards-make-the-difference/

#### *2.3.5. Unsustainability*

The Report discusses vendor lock-in as a factor that may undermine the sustainability of DPI. However, the brief description prevents the Report from effectively capturing this threat. We recommend addressing the:

- Vague use of language: The Report states that vendor lock-in "limits flexibility and adaptability to new technologies, leading to long-term costs and **other challenges**." The phrase in bold lacks specificity, failing to appropriately capture the threat of vendor lock-in. Vendor lock-in can give foreign entities control over sensitive personally identifiable information about a country that local governments may not have access to. For instance, the Nigerian administration was locked out of a critical database with biometric information of Nigerians that was captured in 2004. Foreign vendors were responsible for building this database and had denied the Nigerian government access despite multiple attempts at negotiations. The government ultimately determined it was more sustainable to invest in and build their own database and system.[32] In addition to the high costs incurred due to vendor lock-in, sensitive information about Nigerians was controlled by a foreign entity. Non-specific language prevents the Report from capturing the severity of this risk.

### *2.4. When? The Iterative DPI Life Cycle*

#### *2.4.1. Development*

The Report's discussion of development correctly highlights that local developers should facilitate DPI implementation. To articulate the importance of local capacity, we recommend:

- Clear rationale for empowering local developers: We recommend including specific reasons for why local developers may be better suited for DPI implementation in comparison to foreign entities. For instance, China was accused of bugging and downloading data from servers it built for the African Union headquarters.[33] While both parties have denied these claims, Paul Kagame (former Chairman of the African Union) stated that Africa, instead of China should have built the headquarters. The rationale here may be that local institutions have a more genuine interest and stake in effecting change, in comparison to foreign entities.[34] The rationale and significance of empowering local developers should be explicitly stated in the Report.

### *2.5 Adopting the Framework*

This section offers recommendations to "realise the intended potential benefits of the Framework and prevent societal harms…" It highlights that the Framework is "particularly

---

[32] Asadu, C. (2020). *NIMC: How foreign vendors locked us out of previous database of Nigerians.* The Cable. https://www.thecable.ng/nimc-how-foreign-vendors-locked-us-out-of-previous-database-of-nigerians/
[33] The Guardian. (2018). *China rejects claim it bugged headquarters it built for African Union.* https://www.theguardian.com/world/2018/jan/30/china-african-union-headquarters-bugging-spying
[34] Massally, K., Matthan, R., & Chaudhuri, R. (2023). *What is the DPI Approach?* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/05/what-is-the-dpi-approach?lang=en

useful when building stakeholder capacity, conducting periodic assessments, and improving DPI governance to proactively mitigate risks and harms."

While these are undoubtedly important for the Framework's adoption among those responsible for designing and implementing DPI, their value in the DPI context and connection to the risks and structural vulnerabilities is not stated.

#### *2.5.1. Building Capacity*

This section presents two main issues. First, the Report does not define what building capacity entails, both generally and in the context of DPI. Second, while it highlights the benefits of building capacity, it does not clearly explain its necessity by demonstrating the risks or harms that can arise from the lack of capacity among Responsible Authorities.

For example, many countries face shortages of technical skills within their governments, which limits their ability to design, implement, maintain, monitor, and evaluate the progress of DPI at various stages. Furthermore, such shortages push governments to rely on external assistance to build and implement critical DPI, which weakens the government's control over its public service delivery systems and raises concerns of digital sovereignty. Therefore, building appropriate strategic technical capacity among stakeholders involved in DPI implementation is crucial to prevent costly, ineffective, and unsustainable outcomes. Furthermore, enhancing such capacity can build trust and credibility between public institutions and other stakeholders, helping to reduce digital distrust and encouraging broader adoption of DPI.[35]

[35]Ganapathy, S., Sippy, T., Sinha, V., & Adarkar, H. (2022). *Building the Foundations: Strengthening Technical Capacity for Digital Public Infrastructure in Government.* Artha Global. https://artha.global/reports/building-the-foundations-strengthening-technical-capacity-within-government/