Submitted June 26, 2024

CCIA Submission to the United Nations on the Interim Digital Public Infrastructure Safeguards Report

1. Please select the number that best represents your opinion by indicating the degree to which you agree or disagree with the following statements (1 - Strongly Disagree, 2 - Disagree, 3 - Neutral, 4 - Agree, 5 - Strongly Agree):

a. The first interim report lays out clear arguments for the DPI Safeguards Initiative.

3

b. The emerging framework in the first interim report lays out clear safety and inclusion risks associated with DPI implementations.

3

c. The emerging framework in the first interim report lays out mitigation mechanisms to be adopted during DPI implementations.

4

d. The first interim report was easy and coherent to read.

5

2. Please identify any specific areas or arguments within the report that you found unclear or convincing.

1. An overarching concern with promoting DPIs is that the concept remains inchoate, making it very difficult to evaluate the appropriateness of broadly-applicable and prescriptive policy recommendations. As a general matter, policies appropriate for what are widely recognized as governmental functions (e.g., payment of taxes or access to government services or benefits) are unlikely to be appropriate for functions the private sector delivers efficiently. And, the nature of what is considered exclusively governmental changes over time: for example, telecommunications was once considered a quintessential public infrastructure, but government ownership and management of that sector is now recognized as having greatly undermined its affordability and technological development. Cabinning in these principles and recommendations to cases of demonstrable market failure, or where public-private partnerships can more fairly and efficiently address an unmet need, should be a clearly-articulated premise for any recommendations.

2. The report's focus on various forms of sovereignty and market distortion also requires further clarification. First, overall, the tone of this report appears to suggest that corporate accountability is the overarching solution to addressing risks that authoritarian governance poses to human rights. Safeguards are critical to responsible deployment of DPI, when appropriate and the market dictates its necessity, however, safeguards at the UN level should be focused on guidelines to ensure governments do not abuse digital infrastructure to implement authoritarian governance models. Second, on data sovereignty, the report asserts without evidence on page 19 that DPI without data localization risks violating human rights. Such an assertion contradicts the previous arguments on human rights that recognize the risk of state authorities' accessing individual data, while mischaracterizing the privacy protections offered by modern data storage and transfer offerings. Third, on technological sovereignty, the report cites "dependencies on large foreign technological companies for cloud services" as a risk resulting in "vendor lock-in, high service delivery and use costs, and interoperability challenges… [and] supply chain risks." This argument seems to champion protectionist measures to impede foreign vendors' participation in domestic cloud offerings, without acknowledging the negative effects of such a policy on privacy, innovation, cybersecurity, and market competitiveness. In fact, there are numerous examples of where efforts to mandate indigenous cloud offerings have had precisely this effect (e.g., France's SecNumCloud regime). While ensuring proper safeguards to avoid discrimination and ensure privacy is appropriate, the Safeguards Report should avoid encouraging country-specific requirements that risk hampering rather than enabling innovative digital offerings. Although the report looks to help promote indigenous development of DPIs, it should also ensure that any principles looking to promote or favor local suppliers is consistent with the country's international trade obligations, where, typically, discrimination in favor of local suppliers is proscribed. For example, the implicit endorsement of promoting local cloud computing alternatives must take into consideration countries' obligations in the WTO, under which 75 countries are already obligated to allow foreign suppliers, without discrimination, to offer data processing services.[1] Any principle favoring indigenous cloud suppliers, at the expense of foreign suppliers, would be inconsistent with such obligations and should not be endorsed in a UN document. Fourth, on cyber sovereignty, the report correctly identifies the risk that cyber threats pose to DPI, and the importance of robust cybersecurity protocols to ensure the integrity and privacy of digital infrastructures. National data protection authorities should work with private sector actors to determine context-specific frameworks for protecting user data, and leverage existing international cooperative mechanisms, such as the networks developed by national CERT authorities.

[1] https://www.wto.org/english/tratop_e/serv_e/computer_e/members_computer_services.pdf

3. In section 3 on DPI Opportunities: How accurately does the report capture the potential benefits and risks associated with DPI? Are there any additional opportunities or risks not addressed?

As noted above, this question cannot be precisely answered in the absence of a clearer definition of the scope of DPIs the principles apply to. In general, CCIA views DPI as an evolving concept that may not be relevant to all markets, and therefore should be implemented only when needed to correct for market failures, as opposed to situations where existing solutions are provided by the private sector. As such, multilateral initiatives should not seek to apply DPI universally, but instead support specific applications where existing offerings are lacking. Thus, potential benefits and risks are highly market- and technology-specific. For example, if a country implemented a DPI and ended up mandating a specific technology, it could lock its consumers into a solution that soon became obsolete, or at least sub-standard, and hindered effective competition. This has often happened: for example, Mexico’s failure to allow for the latest generation of payment message formats has meant that Mexican consumers have been denied a range of payment functionalities available in other markets. However, this is not to say there are not valid instances where DPI can be reasonably implemented to provide critical services, as seen with e-payment systems developed during the COVID-19 pandemic.

Regarding Enabling Inclusive Economic Growth, the specific examples of DPI given - including eKYC, digital signatures, and more - are accurately identified as digital offerings with the potential to efficiently deliver public services and reduce market coordination costs. However, given the ambiguity behind the term Digital Public Infrastructure, and the potential for an overly vague definition to lead to suboptimal applications, the report should more clearly tie specific DPI offerings to inclusive economic outcomes using robust evidence. A more narrow, tested justification for DPI ensures that such offerings, when implemented, are the best approach for providing public services and sustaining development.

On Assuring In-Country Implementation, the report correctly identifies the importance of interoperability and collaboration across countries when implementing DPIs. Developing a local DPI that ends up cutting off consumers from other internationally-available solutions can have a clear downside. However, the report lacks more specific details of how DPI interoperability can be achieved, and should outline specific principles for doing so, recognizing that mandating interoperability in some cases can undermine innovation (e.g., if it requires adherence to a lowest-common-denominator standard that subsequent innovators have improved upon). Strong support for cross-border data flows and interoperability with digital transactions is critical for successful implementation of DPI, and highlights the importance of public-private partnerships in fulfilling DPI’s potential.

4. In section 4 on Need for Guardrails: Considering the operational principles contained within the report's framework, how applicable do you find these principles in the political economy contexts you are familiar with? What factors might limit their applicability? Additionally, how do you think these principles could be modified or contextualized to better suit specific local conditions?

CCIA is familiar with assessing and providing guidance on digital policy across diverse economic and regulatory environments. It recognizes the need for context-specific interventions, while maintaining the importance of regulations that encourage cross-border digital flows and limit regulatory fragmentation. As such, Guardrails should allow for context-specific tailoring while ensuring general adherence to principles of regulatory interoperability and the potential for close-collaboration with industry offerings.

Regarding Section 1 on Human Rights Violations, CCIA is a strong proponent of protecting data through robust, technology-neutral frameworks that manage privacy risks for both individuals and organizations. Such approaches are especially critical given the risk that DPI, especially digital ID and data transfer and storage, pose serious potential risks for abuse. DPI, whether publicly or privately operated, should adhere to strong guidelines to safeguard user privacy, protect data, and promote responsible use of AI. Such an approach is critical across all contexts, although close collaboration with private sector actors can help develop innovative, privacy-preserving solutions that are best suited to local contexts. Absent such strong language and protections, overly intrusive digital ID systems and data storage regulations can easily be abused by governments, risking widespread human rights abuses. Governments have already implemented digital ID systems and data storage and transfer regimes that are exploited for surveillance and repression, going beyond the existing harms of discrimination and exclusion detailed in the report. For example, China's data governance regime uses data localization requirements and cybersecurity reviews to justify censorship,surveillance, and "social credit" ranking of individuals, highlighting the risks of DPI offerings absent strong safeguards.

Regarding Section 2 on Market Distortions, CCIA holds the view that the role of DPI is to enhance public service delivery, not influence market competition, with such actions best being left to national competition regulators. The overarching justification, that market power concentration by digital firms harms individual rights and market outcomes, is not fully explained nor demonstrated by a market analysis, and risks diluting the meaning of DPI while endorsing overly intrusive policy outcomes that hamper innovation and public service delivery. In fact, introducing a mandatory DPI in an already well-functioning market risks creating a market distortion of its own. For example, for the ostensible reason of bolstering its sovereignty interests in payment systems, Vietnam recently introduced a national switching system through which most payments were required to transit. In addition to raising privacy issues, Vietnam essentially created a new monopoly service, which disadvantaged private suppliers (both local and foreign) and undermined technological development and cybersecurity safeguards.

In reference to the report's mentions of services and consumer protections, CCIA agrees with the importance of limiting barriers to entry and enabling market demand to drive innovation, but cautions against using DPI as a vehicle for competition policy, beyond the authority of traditional regulatory bodies.

In reference to market distortion risks, CCIA agrees with the references to interoperable standards. However, it recommends that the authors consider the potential for proprietary technologies to enable DPI solutions, in addition to open standards. The term open standards in the context of DPI requires further clarification, and the authors should consider the strong potential for proprietary solutions to offer transparent, scaleable, interoperable, and innovative DPI offerings.

5. In section 5 on Actionable Framework: In the report, strategies for operationalizing DPI risk mitigation are detailed. How do you evaluate the practicality of these strategies for implementing the principles in the contexts you are familiar with? Which aspects of these strategies do you find particularly effective or inadequate? Furthermore, from your experience, are there alternative strategies that could offer more robust solutions for operationalizing these principles to manage DPI risks?

Under Operational Principles, the report effectively identifies the importance of mixed public- and private-offerings to drive innovation and provide DPI. In terms of operational principles, recommendations 1 (leverage market dynamics), 3 (ensure data privacy by design), and 4 (assure data security by design) offer the most practical, impactful solutions. Recommendation 5 (ensure data protection during use) should include more specific language about safeguards from government surveillance. On references to private sector involvement throughout this section, the report should reference both open standards and proprietary solutions to best align with language on leveraging private sector capabilities.

6. Are there any critical aspects or perspectives that you believe are missing or underrepresented in the report?

CCIA believes that the working group should further consult diverse private sector firms, to better capture the opportunities and barriers facing industry in innovating and scaling DPI solutions. Such actors could best report on realistic safeguards for specific DPI offerings, as well as the risks of excessive government intervention on efficient, innovative solutions. Existing DPI rollouts have shown the strong potential for industry to provide financial investments, technological innovation, expertise, capacity building, and strategic partnerships, especially in the context of countries where government institutions lack sufficient funds or skills to do so independently.[2]

7. In the context of multi-stakeholder processes for implementing DPI, which stakeholders are most well-represented and/or have the most influence and which are under-represented and/or have the least influence in your experience?

N/A

8. Any additional recommendations or suggestions as DPI safeguards WG move to the deductive phase?

N/A

[2] https://www.csis.org/analysis/advancing-digital-transformation-and-digital-public-infrastructure-role-private-sector