

Response to Public Consultation on the ‘Indian Artificial Intelligence Stack’ released by the AI Standardization Committee, Department of Telecommunications

IT for Change

October 2020

Introduction

The ‘AI Standardization Committee’ of the Department of Telecommunications (Committee) has taken a necessary step in artificial intelligence (AI) governance by recognising the importance of ‘standards’ to solve potential challenges that may emerge from the deployment of AI solutions. The presentation of a broad framework for these standards, through the paper titled ‘Indian Artificial Intelligence Stack’ (the Paper), will be helpful in framing future discussions on creation of guidelines or regulations by the Government of India as the technology continues to mature.

IT for Change’s comments in relation to the Committee’s framework is divided into two sections. The first section provides general comments applicable to the Paper as a whole. The second section consists of specific clarifications/comments pertaining to design dimensions of the various layers of the Indian AI Stack. We have made reference to relevant paragraph (para) numbers of the Paper, for ease of consideration.

A. General Comments

1. We believe that this Paper does not accurately articulate the potential challenges of AI adoption in various sectors outlined in Section 2.5, and does little to try to link them to the framework being proposed. Furthermore, the scope of enforcement of the framework is unclear and the paper does not describe how the Committee plans to take this idea forward or the governance structures required to do so.
2. The Paper acknowledges the critical role that AI standards development can play in mitigating bias, discrimination, exclusion, and lack of transparency and accountability in automated decision making, and encouraging AI innovation. However, it fails to effectively outline the overarching institutional framework that will ensure these concerns are addressed in the development of the 5 layers of the Indian AI stack (infrastructure, storage, computational, application, data/information exchange layers and the cross-cutting security and governance layer). Further, para 4.20 flags, tentatively, the need for an independent agency to formulate rules/establish boundaries around the Indian AI stack. The idea of an independent agency requires

greater elaboration as it is a very significant part of the larger institutional governance framework.

3. It is unclear how the Indian AI Stack will be built, if it is intended as a digital public good or an enabler for new AI solutions to be developed in the future. The Paper also does not clarify if the Indian AI Stack is to be built and subsequently used by any and all organisations engaging with AI technologies or whether it is a proposed model only for organisations in India engaging with AI technologies.
4. The absence of the above details makes it difficult to analyse and provide comments on the technical framework itself. The Committee recognises the need for standards to be defined across distinct 'layers' of the AI solution value chain, but the technical prescriptions made within the framework are poorly justified - making it difficult to understand the rationale behind technical design choices and engage with them meaningfully. Further, without such justification, enforcement of standards - especially those pertaining to open technology development - can serve only to disproportionately benefit large technology companies.
5. In multiple sections (paras 4.17 5.14, 5.21, 6.1 (c), 7.2.1), the Paper alludes to the inclusion of 'private' data and industry standards, but it is unclear how the framework would interface with private sector entities and their internal development practices, and how these recommendations would be implemented in the public sector. Despite attempting to lay down technical norms to be followed, the Committee only cursorily describes potential institutional structures required for their implementation (by means of Section 6 of the Paper). Therefore, this raises the question of what stakeholders the framework will include within its ambit as well as what enforcement mechanisms will be used to implement the framework and the accompanying standards. It is necessary that these be elaborated upon.
6. While the efforts and intentions of the Committee in laying down standards are appreciated, there is no mention of how the standards of the Indian AI Stack envisaged by the Paper will be reconciled with AI standards being developed in organisations such as the Bureau of Indian Standards (BIS) and Institute of Electrical and Electronics Engineers (IEEE). Given that these efforts are seeing significant government and industry participation, we urge that there be reconciliation between these efforts and the standards within the Paper to avoid both unnecessary duplication as well as conflicting norms, which would defeat the entire purpose of standardisation.
7. The Paper mentions, at para 5.3 that *"In the absence of a clear data protection law in the country, EU's General Data Protection Regulation (GDPR) or any of the laws can be applied. This will serve as interim measure until Indian laws are formalised."* This is highly problematic. It is imperative that a Personal Data Protection legislation is in

place before the Indian AI Stack is operationalised. Without enacting a law, there can be no enforceability of privacy guarantees.

B. Specific comments and clarifications with respect to the design of the various layers of the Indian AI Stack:

Paragraph No.	Relevant text	Comment / Clarification
Figure 1	Data/Information Exchange Layer	The figure has placed “Digital Rights & Ethics Standards” in the Data/Information Exchange Layer. However, issues of digital rights and ethics exist across all layers of the envisioned stack, as has been noted by the paper in para 5.25. Given this, it is unclear as to why the figure places digital rights and ethics standards only in the data/information exchange layer and not across all layers.
5.3	Typically there could be different Tiers of consent be made available to accommodate different tiers of permissions.	It is unclear how this (data/information exchange) layer will be governed, by whom it will be governed, or how differential tiers of permission will be put in place for processing of personal data and non-personal data.
5.15	...The protocols and the interfaces for Hot Data/ Cold Data/ Warm data and the fashion in which they are stored will be defined to ensure how fast the data is accessed.	The rationale behind choosing the “Hot/Cold/Warm” framework is unclear. Independent solution developers will optimise for efficient data querying on a use case basis and it is unclear how or why the Committee intends to impose a common framework on all applications, whether private or public.
5.21	The layer will ensure setting up of a common data controller.	The definition of a ‘data controller’ is unclear. The roles and responsibilities of the data controller, and the legal-institutional basis for the controller’s authority, are also not elaborated.