



## **Access Now's Feedback on the "AI Governance Guidelines Development Report"**

We thank the Ministry of Electronics and Information Technology (MeitY) for the opportunity to provide formal comments on the "AI Governance Guidelines Development Report" and to participate in the roundtable discussion "Ensuring AI Safety: Building a Safe and Trusted AI Ecosystem in India" held by MeitY on 7th October 2024. Below, please find our brief comments on the Report.

### *About Access Now*

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence and expertise based in over 20 countries across six continents, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights.<sup>1</sup>

Access Now engages with a global community of individuals from over 162 countries in our annual RightsCon summit series, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We helped found the Computer Incident Response Center for Civil Society (CiviCERT) network and are a member of the Forum for Incident Response (FIRST).<sup>2</sup> We have special consultative status at the United Nations.

In India and globally, Access Now has consistently engaged with stakeholders including governments and regulatory authorities on matters pertaining to digital rights. Access Now has engaged extensively with international, national, and regional efforts to govern AI and this submission draws on the recommendations from some of the following. We submitted comments on the recent proposed National Strategy on AI in Sri Lanka,<sup>3</sup> AI Basic Law proposal in Taiwan,<sup>4</sup> participated in the negotiation and drafting of the European Union's AI Act,<sup>5</sup> and have engaged with the United Nations (UN) General Assembly resolution "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development."<sup>6</sup>

---

<sup>1</sup> Access Now, *About us*, <https://www.accessnow.org/about-us/>.

<sup>2</sup> CiviCERT, *About CiviCERT*, <https://www.civicer.org/about/>; Forum for Incident Response, *Vision and Mission Statement*, <https://www.first.org/about/mission>.

<sup>3</sup> Access Now, *Submission on Sri Lanka's draft National Strategy on AI*, <https://www.accessnow.org/wp-content/uploads/2025/01/Comments-on-Sri-Lanka-draft-National-Strategy-on-AI.pdf>.

<sup>4</sup> Access Now, *Submission of initial inputs on preview of the draft of the "Artificial Intelligence Basic Law"*, [https://www.accessnow.org/wp-content/uploads/2024/09/Submission-to-Taiwan-AI-Basic-Law-consultation\\_September-2024.pdf](https://www.accessnow.org/wp-content/uploads/2024/09/Submission-to-Taiwan-AI-Basic-Law-consultation_September-2024.pdf).

<sup>5</sup> Access Now, *The EU AI Act: a failure for human rights, a victory for industry and law enforcement*, <https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/>.

<sup>6</sup> Access Now, *Joint statement: Finding the good in the first UN General Assembly resolution on artificial intelligence*, <https://www.accessnow.org/press-release/un-resolution-on-artificial-intelligence/>.



## Comments on the AI Governance Guidelines Development Report:

1. Taking a proactive approach to AI governance.

We appreciate that governing the use of AI will be driven by the need to prevent and “minimise risks and harms” (as stated at page 3 of the report). We recommend that in addition to this prevention-oriented approach, governance should be anchored in proactive goals, such as the strengthening of people’s rights and opportunities for innovation. This would serve as an overarching objective propelling the innovation and governance of AI.

2. Importance of balancing the need for privacy-protecting and comprehensive data sets.

Where “access to much larger datasets for the purposes of training AI systems” is identified as one of the developments that have brought AI into the spotlight, we suggest recognising the issues that often arise with these training datasets. Even though they are large, they are often not diverse enough to enable the AI to compute well-balanced and well-represented outcomes; and privacy and meaningful consent related concerns in respect of the personal information populating these training datasets remain a concern.

3. Strengthening the AI Governance Principles.

We strongly support the adoption of the AI Governance Principles listed in the report, and particularly welcome the emphasis on the impact of AI on people and their rights. To strengthen this approach, we suggest:

- a. In *Transparency*, adding a reference to “meaningful information” including information about the nature and type of training datasets that were used to train the model. Further, in recommendation 5 requiring voluntary and baseline commitments on AI disclosures including transparency reports and disclosures of intended purpose, we strongly recommend that such commitments be made mandatory and not optional for government actors as well to ensure that the public sector remains accountable for its use of technology.
- b. In *Safety, reliability, and robustness*, adding an explicit mention of the need to establish feedback mechanisms for researchers, users and other stakeholders to report errors and inconsistencies, in order to help with achieving the goal of mitigating and resolving risks and adverse outcomes.
- c. In *Inclusive and sustainable innovation*, adding a requirement of ensuring that environmental impact assessments are conducted and harms are mitigated. The growth of AI and linked data centers has also resulted in risks for the environment and climate. Adding this express language would help set a proactive, forward-looking agenda that serves as a precedent for the global majority and beyond.



4. Creating mechanisms for accountability and managing harms without hurting privacy and security measures.

While some technical tools can help to mitigate harms arising from the use of generative AI technology, some measures are not always best suited to all platforms. Specifically, with reference to traceability being an example of a technological measure enabling compliance in the context of deepfakes, we respectfully urge that this specific measure not be considered for end-to-end encrypted (E2EE) platforms. Implementing traceability, and assigning a unique identifier to each user and tracking chains of communications, would compel E2EE platforms to fundamentally alter their architecture, ceasing to be able to provide the privacy and security for which people rely on them. There are several alternatives, including stronger on-platform reporting mechanisms, content provenance initiatives that allow users to verify the veracity of a file and so on. This would also be aligned with the overall focus in the report on protecting fundamental rights, including free expression and privacy.

In this context, we also recommend Access Now's discussion paper on the effectiveness and appropriateness of watermarking as a tool to further rights.<sup>7</sup>

5. Implementing the AI Governance principles should be done with consultation of all stakeholders.

As the report rightly identifies, it is important to take a holistic approach, and keep an eye towards governing the entire ecosystem as a whole. Operationalisation of the governance principles, as well as any further steps on modifying and finalising them, should include consultations and collaborations with a wider range of stakeholder in addition to government and industry, including academics, civil society, researchers and subject matter experts.

The Inter-Ministerial AI Coordination Committee sought to be established should also take input from a wide range of stakeholders, including academics, civil society, researchers and subject matter experts. This will ensure that governance principles, and the whole-of-government approach more broadly, is informed by diverse and cross-sectoral perspectives and expertise, and are therefore more suited for the long-term and varying use-cases.

6. Public awareness and engagement is key for the successful adoption of the AI incident database.

---

<sup>7</sup> Access Now, *Identifying Generative AI Content: When and How Watermarking Can Help Uphold Human Rights*, <https://www.accessnow.org/wp-content/uploads/2023/09/Identifying-generative-AI-content-when-and-how-watermarking-can-help-uphold-human-rights.pdf>.



We recommend that MeitY work with diverse stakeholders on developing a model for enabling public awareness of and engagement with the “AI incident database”. This should be done in a manner that enables transparency, solicits feedback, invites scrutiny and accounts for periodic reviews and consistent improvements. This will also help strengthen research and accelerate innovation of dependable systems.

7. Improving industry engagement with relevant stakeholders will make the AI governance frameworks more relevant and need-specific.

We recommend that industry groups be required to conduct inclusive consultations in the process of developing the recommended voluntary commitments. Commitments engendered in silos will not fully prevent against the risks and measures that other stakeholder groups have the experience and expertise to identify and recommend. In this context, we welcome the push towards the elements set out on page 12, including regular transparency reports by AI developers and deployers, commitment to enable peer review, testing and monitoring data quality and conducting security and vulnerability assessments. Information security researchers around the world have played an important role in helping service providers identify risks and gaps, and we suggest that companies be urged to establish mechanisms to enable such feedback. Further, the commitments should include an explicit prioritisation of users’ autonomy and privacy.

We remain committed to continuing to engage with MeitY, industry, and all stakeholders involved in trying to develop an exemplary model of AI governance in India, and would welcome opportunities in this regard, including in the form of engagement with the “AI Sub-Group” recommended in the report.

Yours sincerely,

**Shruti Narayan**

Asia Pacific Policy Counsel

[shruti@accessnow.org](mailto:shruti@accessnow.org)

**Namrata Maheshwari**

Senior Policy Counsel and Encryption Policy Lead

[namrata@accessnow.org](mailto:namrata@accessnow.org)

**Raman Jit Singh Chima**

Senior International Counsel and Asia Pacific Policy Director

[raman@accessnow.org](mailto:raman@accessnow.org)

**Access Now** | <https://www.accessnow.org>