

DSCI's Response to NITI Aayog's Discussion Paper on Responsible AI Use of Facial Recognition Technology (AIFRT)

The Data Security Council of India (DSCI) submitted its considered feedback on NITI Aayog's third publication in the Responsible AI series, titled **"Responsible AI for All: A Use Case Approach on Facial Recognition Technology (FRT)"** released in **2022**. With prevalent discourse on ethical AI deployment, and a specific focus on Facial Recognition Technology (FRT), DSCI acknowledged NITI Aayog's commitment to fostering responsible, safe, transparent, and accountable AI use in public sector applications. While broadly supportive of the paper's recommendations, DSCI Policy Team highlighted key areas requiring further safeguards, clarification, and policy development.

DSCI emphasized the criticality of consent and data subject awareness in the deployment of FRT. It raised concerns regarding the unregulated creation and use of facial datasets without the knowledge or consent of individuals. The response argued for stricter controls to curb the unethical or illegal collection of biometric data. Although the Data Protection Board of India would hold authority to direct urgent mitigation measures, DSCI noted that the current legal framework lacks adequate scope, especially in cases involving extra-territorial data processing or when privacy harms were narrowly defined.

The paper's observation that datasets collected for one purpose were being repurposed for others was supported by DSCI. It reiterated that informed consent was foundational to a robust data protection regime and warned that overly broad interpretations of consent—particularly for data sharing and repurposing—could undermine privacy protections enshrined in law. Furthermore, DSCI recommended a differentiated regulatory approach based on the specific function of FRT systems (e.g., 1:1 authentication versus 1:n identification), noting that the nature of deployment should influence legal obligations.

In its comments on digital public spaces, DSCI drew attention to prevailing assumptions that data posted online—even in semi-private forums—could be treated as public. This interpretation, it cautioned, risked legitimizing mass surveillance practices under the guise of public data access. It called for further clarification and safeguards in such contexts. DSCI also flagged gaps in the paper regarding the collection of facial data for gallery datasets, especially for live FRT applications. The organization called for more detailed analysis on consent mechanisms and the ability of data subjects to exercise rights. Importantly, DSCI pointed out the absence of any discussion on the unique risks posed to children, despite some state governments using FRT to trace missing minors. It urged that child data be given special attention in any supplementary materials or future regulations.

To address these concerns, DSCI proposed several policy interventions. These included the adoption of soft legislation in the form of guidelines that set accuracy

thresholds, context-specific deployment rules, and transparency norms. It advocated for technical safeguards and a comprehensive oversight mechanism comprising independent supervision, legal authorization, audits, and grievance redress. DSCI also recommended the use of technical standards and the establishment of regulatory sandboxes to allow safe, controlled experimentation of FRT use. These environments, monitored by data protection authorities, would promote innovation while ensuring accountability, flexibility, and the protection of individual rights. Through this submission, DSCI reiterated its commitment to advancing ethical, privacy-conscious, and human-centric AI frameworks in India.