Feedback on Proposed Amendments to

The Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020

Submission by IT for Change

May 2023

IT for Change

Feedback on Proposed Amendments to The Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020

IT for Change,[1] May 2023

IT for Change's Response:

1. The amendment is not justifiable under the parent Act in its current form: The current amendment will allow most, if not all, commercial digital platforms to insist on Aadhaar authentication from users for a wide variety of services – for example, e-commerce platforms, ed-tech, fintech, security platforms, hospitality platforms like online hotel booking services, etc. – under the guise of promoting ease of living.

It not only opens up a range of risks pertaining to data privacy violations but is also *ultra vires* to the parent legislation, the Aadhaar Act 2016. There is no mandate in the 2016 Act to support any amendment that enables private entities to deploy Aadhaar authentication in service provisioning. Under Section 7 of the Act, authentication is permissible only for the Central or State government for the provision of benefits or subsidies drawn from the Consolidated Fund of India. Also, Section 57 of the Aadhaar Act that allowed for any "body corporate or person" or private entity to demand the Aadhaar ID from citizens for the purpose of identification was struck down by the Supreme Court, and subsequently repealed by Parliament. Against this backdrop, re-introducing the repealed provision through delegated legislation is unjustifiable.

2. The amendment fails the three-pronged proportionality test of the Puttaswamy judgment: The amended Rule 4, in extending the Aadhaar authentication to private entities, falls short of the Puttaswamy I (2017) proportionality test. The new rule does not measure up, for the following reasons:

a) First, legality can only be established through an Act of Parliament. The Aadhaar Act, 2016 offers no room for the executive to broaden the ambit of requesting entities to include non-state actors.

b) Second, the state is duty-bound to expressly demonstrate that rights-infringing measures (access to sensitive information) are necessary and proportionate to the goal sought to be achieved. It is not clear how Aadhaar authentication to enable ease of access to services provided by private entities will qualify as furtherance of good governance (read with Section 7 of the Aadhaar Act). Thus, the state also fails to establish proportionality.

[1] This submission is developed by Anita Gurumurthy, Nandini Chami, Shreeja Sen, and Eshani Vaidya of IT for Change.

3. The amendment poses grave risks to privacy in the absence of a data protection regime: The absence of a clear data protection ecosystem backed by law puts individuals at risk on questions of privacy in several ways:

a) Civil society organizations and digital rights activists in India have raised concerns about how the amendment will enable private entities to access personal data, which in the absence of guardrails could compromise data security and privacy. In the absence of personal data protection legislation, there is no recourse for citizens in case of identity theft and data breaches. There is also an intensified risk of profiling as requesting entities can now track an individual's activities across multiple domains of service using Aadhaar's functionalities as a universal digital identifier.

b) Further, the Aadhaar regulatory ecosystem does not provide individuals the express right to opt out of the scheme. This makes the Aadhaar authentication system mandatory, and not voluntary.

4. The amendment poses the risk of private entities not receiving sufficient scrutiny by the Unique Identification Authority of India (UIDAI): The Comptroller and Auditor General (CAG) of India's Audit Report on the Functioning of Aadhaar has noted that the UIDAI did not comply with provisions requiring the UIDAI to conduct audits and checks for requesting entities under the Aadhaar (Authentication) Regulations, 2021. Given this track record, there is a lack of accountability for private firms who apply to be requesting entities for Aadhaar authentication.

5. The amendment fails to provide accountability and redressal mechanisms: With non-state actors, especially for-profit, private entities being permitted to offer authentication services, citizens are left vulnerable to privacy-related and exclusionary harms. The current Aadhaar authentication system does not provide for a responsive grievance redressal mechanism for data breaches and rights violations. The amendment does not expressly provide for a redressal mechanism, nor does it reference one. The CAG's Audit Report (2021) reflected delays in the current grievance redressal system, in addition to reports of several complaints at the Regional Office level not being escalated to UIDAI (HQ). In the case of the fundamental right to privacy, its enforceability against private entities is also not available. This requires urgent and immediate attention by the state and UIDAI, respectively.