



THE INDIAN SUPREME COURT'S AADHAAR RULING: MIXED NEWS FOR INCLUSION

OCTOBER 9, 2018

CONTEXT AND OVERVIEW

On September 26, 2018, in a 1,448-page [judgement](#), the Supreme Court of India declared [Aadhaar](#) – the Indian government's (and world's largest) digital ID system – constitutional. The system, which emerged in 2009, looks to assign each resident of India a unique 12-digit number linked with the individual's biometric and demographic data and has reached more than 1.2 billion people.

Aadhaar's goal, put simply, is inclusion. The government hopes that by helping individuals establish identity easily, reliably, and securely, Aadhaar will increase participation in beneficial services provided by government entities and private companies. This laudable vision has faced setbacks over the years, with numerous widely documented incidents raising concerns about state surveillance, privacy more generally, misuse, and the exclusionary effect of *mandating* Aadhaar for certain services.

The Supreme Court, grappling with these and other concerns, upheld Aadhaar but with caveats (with one of five Justices dissenting). The ruling and its implications could provide valuable insights to other countries' governments working on ID systems.

As explained below, parts of the ruling could aid Aadhaar's vision of inclusion; others could significantly undermine it.

POTENTIALLY AIDING INCLUSION

- *For several services, Aadhaar is no longer mandatory.* While the *option* to use Aadhaar to participate in services can boost inclusion, *mandating* Aadhaar (i.e., prohibiting individuals from using other forms of ID) can undermine inclusion for several reasons, including the infrastructural and logistical [challenges](#) of Aadhaar enrollment and implementation. The Court ruled (on multiple grounds) that Aadhaar is no longer mandatory for a variety of services, including bank accounts, mobile phones, and examinations and admissions at educational institutions.
- *Individuals have enhanced privacy and control.* The Court prescribes numerous measures that limit the government's powers and bolster an individual's privacy and autonomy in the context of Aadhaar.

ABOUT ASG

Albright Stonebridge Group (ASG) is the premier global strategy and commercial diplomacy firm. We help clients understand and successfully navigate the intersection of public, private, and social sectors in international markets. ASG's worldwide team has served clients in more than 110 countries.

These measures include:

- The government must not retain authentication records beyond six months (as opposed to the earlier limit of five years);
- The government must not retain metadata regarding authentication transactions;
- If the government seeks the disclosure of an individual's information (including identity information and authentication records), the court reviewing the government's request must provide the individual a hearing;
- Disclosure sought on national security grounds requires judicial scrutiny;
- Individuals can file complaints regarding non-compliance with the Aadhaar Act (the statute governing Aadhaar), extending this right beyond just the UIDAI (the Unique Identification Authority of India, the government body implementing Aadhaar); and
- Offering the use of Aadhaar for a given service must be backed by law, and that law is subject to judicial review.

SIGNIFICANT RISKS TO INCLUSION

- *The private sector may no longer be able to leverage Aadhaar.* Citing concerns regarding data privacy and misuse, the Court's decision appears to ban private companies (Indian and international) from using Aadhaar to authenticate individuals who use their services.
 - This can undermine inclusion in multiple ways. For example:
 - It can significantly raise authentication costs for the numerous private companies – especially telecom operators, fintech firms, and small and medium enterprises (SMEs) – who rely on Aadhaar's quick and cost-effective authentication mechanism to provide beneficial services (including sometimes services related to government schemes). This rise in costs could transfer to consumers, hamper companies' ability to scale, deter investment and innovation, and consequently hinder inclusion.
 - Private companies may be denied more than just Aadhaar-based authentication. India's technology infrastructure which provides Aadhaar-based authentication provides additional facilities linked closely with this authentication, including cashless financial transactions and paperless document transfers between entities, based on the individual's consent. This infrastructure is called [India Stack](#). The Court's ruling may, to the detriment of inclusion, undermine private companies' ability to leverage India Stack's enormous potential or contribute to its enhancement (including its security).
 - The Court's reasoning for this ban is contentious for several related reasons. For example:
 - The Court's categorical embrace of data privacy and misuse concerns, to outlaw the *private* sector's use of Aadhaar, stands in sharp contrast to the Court's mostly categorical dismissal of those concerns when discussing Aadhaar more generally.
 - Further, the Court's data privacy and misuse concerns could be addressed by the data protection law India is developing (see ASG's May 2018 [analysis](#) and [op-ed](#), and August 2018



[analysis, on that law](#)). That law will govern all collection and processing of individuals' personal data including in relation to Aadhaar. In fact, the Court recognizes this developing law and asks the government to make it robust and enact it urgently. A robust data protection law around the corner renders the Court's ban unnecessarily harsh.

- The Court's ban may have been motivated, at least in significant part, by its desire to justify the controversial way in which the Aadhaar Act (the statute governing Aadhaar) was enacted in 2016. The Act was characterized as a "money bill" (a bill concerning only government expenditure and taxation), and this characterization allowed the bill to sidestep review from the Rajya Sabha (the upper house of India's Parliament), where the government lacked majority. The Court chose to uphold this characterization. Banning the private sector from using Aadhaar may have been one of the Court's means to this end.
- The judgement is somewhat ambiguous, potentially leaving the door open for private companies. Since the ruling, substantial confusion has emerged among observers regarding the Court's intention regarding private companies. While the judgement strongly suggests that (as discussed above) private players are banned from using Aadhaar, the judgement can plausibly be interpreted as permitting private players to use Aadhaar if the government passes a law supporting that use. Relying on this interpretation, the government appears to have begun efforts toward developing such a law. Private companies interested in using Aadhaar should consider actively engaging with stakeholders on this issue.
- *For many critical government services, Aadhaar is now mandatory.* While the Court (as discussed above) declared Aadhaar optional for several services, it declared Aadhaar mandatory for many others. These include primarily government welfare programs – services that often support marginalized sections of the population. Given the logistical and infrastructural [challenges](#) in Aadhaar enrollment and implementation, and that marginalized sections of the population are often particularly vulnerable to these challenges, the Court's ruling risks denying critical services to these sections of the population, further marginalizing them.
- *Concerns regarding government misuse of data persist.* While the Court orders several measures, as discussed above, that help mitigate the risk of the government misusing individuals' information (e.g., for surveillance and other forms of targeting), those measures may be insufficient. This risk is exacerbated by the data protection law India is developing, because that law provides strikingly broad powers to the government (*see ASG's August 2018 [analysis](#)*).

ASG's South Asia Practice has extensive experience helping clients navigate markets across South Asia. For questions or to arrange a follow-up conversation please contact [Nikhil Sud](#).

