INFOLEX
NEWSALERT

OCTOBER 2018

THE SUPREME COURT'S AADHAAR JUDGEMENT AND THE RIGHT TO PRIVACY

1. INTRODUCTION

At the end of September, the Supreme Court of India, in *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.*,[1] upheld the overall validity of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the "**Aadhaar Act**").

The Aadhaar Act was held to be constitutional to the extent it allowed for Aadhaar number-based authentication for establishing the identity of an individual for receipt of a subsidy, benefit or service given by the Central or State Government funded from the Consolidated Fund of India.

However, the Supreme Court disallowed the use of individual Aadhaar numbers by any private entities for establishing the identity of the individual concerned for any purpose pursuant to a contract, on the basis that it was contrary to the fundamental right to privacy. The Supreme Court also ruled on a number of laws, circulars and directions, which required the mandatory linking of Aadhaar for receiving relevant services.

This alert analyses the tests adopted by the Supreme Court, specifically in relation to the right to privacy of an individual, in arriving at the conclusions mentioned above. Further, it briefly discusses the orders passed regarding existing requirements for the mandatory linking of Aadhaar numbers. Finally, the alert analyses the data protection principles recognized by the Supreme Court in this judgement, in light of the Personal Data Protection Bill, 2018 (the "**Bill**").

2. ANALYSIS

2.1 Right to Privacy

The Aadhaar Act entitles resident individuals to obtain an Aadhaar number by submitting certain biometric information and demographic information as part of the enrolment process. Subsequently, each time the identity of the individual is required to be verified by the Government or private entities, the Aadhaar number and biometric information, in some cases, was requested as part of the individual identification process, for authentication. As part of the authentication process, certain transaction details are recorded at a central database, arguably creating the framework for a surveillance state.

The Supreme Court was primarily required to assess if the provisions of the Aadhaar Act were contrary to the right to privacy, which has been established as a fundamental right by the Supreme Court in 2017. In this regard, it is relevant to note that a number of services provided by both private entities and Government, was contingent on an individual linking their Aadhaar number for authentication, which indirectly made it mandatory for most individuals to obtain an Aadhaar number. Therefore, the question

[1] *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.*, available at <https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf> .

was not so much whether this was an infringement on the right to privacy, but whether it was a reasonable exception to it.

The Supreme Court held that the right to privacy cannot be impinged without a just, fair and reasonable law. This required existence of a law, which serves a legitimate state aim and is *proportionate* to the objective sought to be achieved. The Supreme Court further clarified that the *proportionality test* includes the following four aspects

(a) **Legitimate goal**

The measure restricting the right must have a legitimate goal.

(b) **Rational connection**

It must be a suitable means of furthering the goal.

(c) **Necessity**

There must not be any less but equally effective alternative.

(d) **Balancing**

The measure must not have a disproportionate impact on the right holder.

The Supreme Court struck or read down certain portions of the Aadhaar Act, which did not fulfill the above *proportionality test*. However, aside from these provisions, the Supreme Court held that the Aadhaar Act, on the whole, as a law, serves a legitimate state aim and is *proportionate*, thereby being a reasonable exception to the right to privacy.

Section 7 of the Aadhaar Act, making the Aadhaar number mandatory for receiving subsidies, benefits and services from the Government (for which expenditure was drawn from Consolidated Fund of India) was therefore held to be valid.

However, the most relevant provision which was read down by the Court was Section 57 of the Aadhaar Act. This provision allowed Government entities, body corporates and individuals to use the Aadhaar number for establishing the identity of an individual for any purpose, pursuant to any law or contract.

Firstly, the Supreme Court held that the phrase '*any purpose*' is not *proportionate*, too wide and susceptible to misuse. The Supreme Court laid down that the purpose has to be '*backed by law*'.

Secondly, the possibility of collecting and using Aadhaar numbers for authentication pursuant to a contract was disallowed since this may result in individuals being forced to give their consent in the form of a contract for an *unjustified* purpose. The Supreme Court laid down that the contract has to be '*backed by law*'.

Thirdly, private entities are not permitted to use Aadhaar numbers for the purpose of authentication, on the basis of a contract with the concerned individual, since it would enable commercial exploitation of an individual's biometric and demographic information by private entities. This effectively prevents companies from using Aadhaar based e-KYC authentication of an individual's identity, which was primarily the way in which many companies complied with the relevant *know your customer* (KYC) requirements.

2.2 Consequential orders

The Supreme Court was also tasked with deciding the validity of certain directions from different departments of the Government (*brought in through laws or otherwise*), which mandated the linking of Aadhaar numbers to benefit from certain services. This was specifically analyzed in the context of the linking of Aadhaar numbers to Permanent Account Numbers (PAN) (relevant for income tax filings), bank accounts and mobile phone numbers. The Supreme Court noted the following.

(a) The requirement to mandatorily link Aadhaar numbers to PAN was held to be valid, since it was based on a law, serving a legitimate state interest and was *proportionate*.

(b) The requirement to mandatorily link Aadhaar numbers to bank account numbers was held not to be valid since it did not meet the *proportionality test*.

(c) The requirement to mandatorily link Aadhaar numbers to mobile numbers was held not to be valid since it did not serve a legitimate state aim and was *disproportionate* in its encroachment on individual liberties.

2.3 Data Protection Principles

The Supreme Court categorically recognized certain data protection principles such as data minimization (*restricting collection of data to data necessary for stated objects or purpose*), purpose limitation (*limiting the scope of purpose and using the data only for such purpose*), data retention (*retaining the data only for a limited period necessary for the purpose*) and data security as relevant factors in determining whether the provisions of particular legislation, including the Aadhaar Act, was in conformance with an individual's right to privacy.

While the Supreme Court discussed various data privacy principles from the United States and European Union jurisdictions, it did not specify *which* of those principles should be adopted in the Indian context. The Supreme Court also recognized and discussed a number of provisions from the Bill, again without much clarity on *which* of those principles should be imported into judicial reasoning.

4. INDUSLAW VIEW

The most significant and immediate implication of the judgement is for those private companies or body corporates, which are reliant on Aadhaar based customer authentication mechanisms. This is specifically an issue in the context of companies in the *fin-tech* space that are required by sectoral regulators, such as the Reserve Bank of India, to undertake KYC compliance.

Aadhaar-based e-KYC, under the Aadhaar Act, was seen as a means to accomplish the KYC compliance in an efficient paperless manner. It is now expected that the Government or sectoral regulators will bring in alternate mechanisms, which will need to be equally effective in identification of individuals.

In this context, it should be noted that the Employee Provident Fund ("**EPF**") Organization had issued a circular, which required employers to link the Aadhaar numbers of all eligible employees to their respective EPF account. Given that the Supreme Court has held Section 57 of the Aadhaar Act unconstitutional, employers are no longer permitted to collect the Aadhaar numbers of employees for the purpose of linking it to their EPF accounts. Any failure by employers to comply with the Supreme Court ruling will result in employers being in contempt of court.

Finally, the judgment also discussed the Bill, which was noted as including many of the progressive data protection principles inspired by the European Union General Data Protection Regulations (the "**EU GDPR**").

Even though the Supreme Court recognized that there may be scope for further fine tuning of the Bill, it was observed that we are not far away from a comprehensive data protection regime, which entrenches informational and data privacy.

These observations, coupled with the extensive discussion on jurisprudence from the European Union suggests that the courts in India are likely to rely heavily on the principles adopted in EU GDPR in future cases, though there is a lack of clarity on the specific principles that would be imported.

Authors: Namita Viswanath | Savithran Ramesh

Sector: Government & Regulatory |Technology, Media & Telecommunications

Date: October 8, 2018

DISCLAIMER

This alert is for information purposes only. Nothing contained herein is, purports to be, or is intended as legal advice and you should seek legal advice before you act on any information or view expressed herein.

Although we have endeavored to accurately reflect the subject matter of this alert, we make no representation or warranty, express or implied, in any manner whatsoever in connection with the contents of this alert.

No recipient of this alert should construe this alert as an attempt to solicit business in any manner whatsoever.