

## AADHAAR ACT AND ITS PRIVACY CHALLENGES

Written by *Hriday Shah*

*3rd Year BBA LLB Student, NMIMS Kirit P. Mehta School of Law, Mumbai, India*

---

### ABSTRACT

The Aadhaar Act is a money or cash bill of the Parliament of India. Passed by the Lok Sabha on the 11 March, 2016, this bill came into power on 12 July, 2016 and 12 September, 2016. An Aadhaar card is a card given to citizens of India and it reflects the proof of residence of a citizen of India and does not reflect their citizenship as a passport does. It was first conceptualized in 2009 and has been issued since then. It collects biometric data of the citizen such as fingerprints and eye scans and a photograph of the face.<sup>i</sup> A unique 12-digit code is assigned to each person and all this data is stored by the Unique Identification Authority of India or UIDAI in specific servers. These servers are said to be “physically protected” by the UIDAI. All this data is processed, kept and secured in UIDAI’s own server. These servers are not connected to the internet or any pen drive or similar devices. This information was given by UIDAI themselves.<sup>ii</sup> The Aadhaar Card holds various details about the holder of the card such as name, date of birth, address, gender, and name of parents or guardians in case of children.

The Aadhaar Act also has a few similarities with the National Identification Authority of India Bill, 2010. The most notable differences between the NIAI bill and Aadhaar Act are the three member board known as the Identity Review Committee and the section 8 of the Aadhaar Act is wholly different from that in the NIAI bill. Other difference between these two is that Aadhaar collects more data than biometrics which NIAI only collected the biometrics of the individual.<sup>iii</sup> This research paper’s main aim is to analyse if Aadhaar Act is an ambitious plan or a privacy concern. The Bharat Bhushan Gupta case and the Airtel scams have been analysed and studied.

People's perspectives have been highlighted. Data breaches and how they happen in the Aadhaar cases have been explained vividly. Suggestions to the Aadhaar Act and how to make it better have also been stated.

**Keywords:** Aadhaar Act, Aadhaar Card, UIDAI, Privacy concerns to Aadhaar

## RESEARCH OBJECTIVES

The objectives of this study are as follows:

1. To determine how sensitive data might be leaked from Aadhaar details.
2. To compare data security protocols of India to other systems' jurisdictions.
3. To analyse if it is a good plan since data breaches have been increasing yearly.
4. To analyse People's perception of Aadhaar.

## LEGAL ASPECTS

### *How does this sensitive data from Aadhaar leak?*

Aadhaar data is very sensitive and it is very important to be kept private and away from the public to prevent misuse of the data. But, UIDAI has failed to make a secure software that runs Aadhaar. It has secure servers that are "physically protected" but that is not convincing for the data breaches that are happening.<sup>iv</sup> The software that Aadhaar uses is called Enrolment Client Multi-Platform or ECMP.<sup>v</sup> It is open source which means it isn't hidden from the public.<sup>vi</sup> Anyone who knows how a software works can easily find the codes from where data can be stolen. Some even rewrite the code and sell the stolen information for illegal prices ranging from Rs. 500 to Rs. 2000.

### *Comparisons*

When we compare the laws on data protection in India to the ones in UK. In the UK, data protection act is called EU General Data Protection Regulation or GDPR.<sup>vii</sup> The main objectives of GDPR are as follows:

- Protection of people when their data is processed.
- Protection of their fundamental rights and right to freedom of movement for processing purposes.
- Protection of data.

GDPR is ahead of the Indian laws in a few aspects such as protection of the person when their data is being processed. The Indian laws only enable data transfer, not protection. The protection of the person was kept in mind when the GDPR was framed.<sup>viii</sup>

There is also a huge difference between the definitions given by both jurisdictions about the word “processing”. In Article 4 (2) as concrete but no such definition has been given about the term in the Indian jurisdiction.<sup>ix</sup>

### ***Data Breaches***

Right to privacy must be a common right that every individual must have. In 2017, the government of India declared privacy as a fundamental right.<sup>x</sup> Aadhaar Act was one of the main reasons for this verdict since it was the main reason to be worried about one’s privacy.<sup>xi</sup> When the government was asked what they meant by privacy, they answered it was the right of an individual to be left alone and the right to live without the interference of other individuals in such matters that they should be not concerned with.<sup>xii</sup> In 2018, a report showed that Aadhaar had the most data breaches of all. More than 1.1 billion data breaches were conducted against people’s names and their unique Aadhaar card numbers as of March of 2018.<sup>xiii</sup> This begs the question if the Aadhaar Act is a success or a failure since these many data breaches are not acceptable. Millions of people and their data information is available so easily to the public and its misuse is a cakewalk for anyone. According to most of the population, Aadhaar is a trade-off between society and privacy.<sup>xiv</sup>

## **SCENARIO**

### ***Bharat Bhushan Gupta: the first person to debunk the Aadhaar’s privacy challenges***

The Aadhaar Act’s privacy concerns were first picked up by Bharat Bhushan Gupta, a 32-year-old male from Jalandhar. He was a Village Level entrepreneur in Jalandhar and was approached by an unknown entity via the internet messenger application of WhatsApp. The

unknown entity claimed to provide Bharat Bhushan Gupta with the sensitive information and data of people whose Aadhaar card's 12-digit number he would enter. Bharat Bhushan Gupta tried using the access by entering his own Aadhaar number and sensitive data that should not have been authorised to be seen by the public was available. Bharat Bhushan Gupta called the toll-free number provided by the UIDAI which no one answered after multiple attempts to get this to their notice. When they finally answered, they told him that no official was available to look into the matter of data being openly available by paying a small amount. So, Bharat Bhushan Gupta tried to seek the help of the media. He approached The Tribune, who with the assistance of Gupta, verified that what he claimed was true and this made people's concerns rise in terms of privacy challenges and data theft.<sup>xv</sup>

### ***The Airtel Scam***

When it was made compulsory to link phone numbers and the Aadhaar cards of individuals, Airtel, a company providing internet services saw a chance to scam people and open new bank accounts without the consent of the people buying their services. Millions of people collectively reported of more than 47 crore rupees being transferred in a new bank account linked to their number which they were unaware of. Airtel would say they need the phone number of the customer so that they can re-verify it but in turn they would make these new bank accounts. This led to the suspension of Airtel's e-KYC licence. If this would go on, it might have led to unethical and even anti-national actions by people.<sup>xvi</sup>

## **PROBLEMS AND SUGGESTIONS**

When Aadhaar was launched, it of course had many flaws such as it having collected all sensitive data about everyone residing in the country. This is a problem and a concern brought forward by many members of the parliament as it is threatening to the national security of India. These recommendations were listed by the members of the parliament. There are two types of other flaws as well that were unaddressed. (1) Aadhaar can easily and without consent enable the government to access data of the person and (2) problems with the collection of biometric data for 1.2 billion people. The system could only record up to 200 million and there was a chance of not correctly recording the fingerprints of 15% of the people.

A few suggestions given by the Members of the Parliament are:

- The bill stated that authentication by Aadhaar number was not mandatory but it actually was mandatory contradicting what the UIDAI said. So, this point must be stated in the act as well that authentication by Aadhaar number is mandatory.
- So much data cannot be stored for long periods of time in one place, so all this data would need to be transferred. This transfer must happen through highly cryptic methods of data transfer.
- The bill defines “biometric data” very vaguely. It must be explained and defined exhaustively.
- A chain of trust must be incorporated so that if any foreseeable incident ever takes place, one doesn’t blame the technology.
- The residents also must have a few rights such as access and correct information that was collected about them. They must also be notified about any breach in their data.<sup>xvii</sup>

## CONCLUSION

The Aadhaar bill is definitely an ambitious plan but fails in the cases of privacy concerns. Aadhaar connects the Aadhaar card, which is a proof of residence, with their phone numbers and PAN card details. But all this came at the cost of poor security of this data. This privacy concern was picked up first by Bharat Bhushan Gupta who shared his incident and how one offered him data of others at the cost of Rs. 500. Airtel also scammed their customers by creating new bank accounts in their names without their consent by using their phone numbers that were linked to their Aadhaar card. The poor software and easy scamming of people as it is simply getting a phone number and an OTP or One-Time Password. People are also quoting.

Aadhaar as a trade-off: Better for society but bad for the privacy of the person. For the government, they are sceptical about the new right to privacy and are keen on making Aadhaar a success. We can conclude that Aadhaar is just a privacy concern at the cost of a better society. The easy linking with phone numbers and as a proof of residence card costs a person’s privacy.

## ENDNOTES

---

- <sup>i</sup> Diva Rai, An Overview of the legitimacy of the Aadhaar Act by the Supreme Court, iPleaders (Oct. 11, 2020).
- <sup>ii</sup> Aadhaar Data kept, processed only on own secure servers: UIDAI. Economic Times (Aug. 30, 2017).
- <sup>iii</sup> *ibid*
- <sup>iv</sup> Compromised *Aadhaar enrolment software being sold for as little as Rs. 500: Report*, Business Today (Nov. 30, 2021).
- <sup>v</sup> *ibid*
- <sup>vi</sup> Saikat Datta, India's ambitious digital ID project faces new security nightmare, Asia Times (May. 1, 2018).
- <sup>vii</sup> EU General Data Protection Regulation (GDPR) Definition, Trend Micro (2019)
- <sup>viii</sup> Anisha Agarwal, SANCTITY OF PERSONAL DATA: A COMPARATIVE STUDY OF DATA PRIVACY LAWS IN EU, US AND INDIA, The Law Brigade Group 171, 4 (2020)
- <sup>ix</sup> General Data Protection Regulation, art. 4, Cl. 2.
- <sup>x</sup> Right to Privacy a Fundamental Right, says Supreme Court in unanimous verdict, The Wire (Aug. 24, 2017)
- <sup>xi</sup> Krishnadas Rajagopal, The lowdown on the right to privacy, The Hindu (Jul. 29, 2017)
- <sup>xii</sup> Varun Kalra and Ramisha Jain, *An Armistice between right to privacy and right of surveillance*, HeinOnline (2018)
- <sup>xiii</sup> The 20 biggest data breaches of 2018, Dashlane (Jan. 9, 2019)
- <sup>xiv</sup> Ajay Ghangare and Dr. Anup Ranade, *Aadhaar Card – Perspectives on Privacy*, ResearchGate (2019)
- <sup>xv</sup> Rachna Khaira, *Aadhaar Whistle-blower who first called UIDAI*, The Tribune (Jan. 6, 2018,)
- <sup>xvi</sup> Anand Venkatanarayana and Shrikanth Lakshmanan, *Aadhaar Mess: How Airtel pulled off its Rs. 190 crore magic trick*, The Wire (Dec. 21, 2017)
- <sup>xvii</sup> Amber Sinha, et al. List of Recommendations on the Aadhaar Bill, 2016 – Letter submitted to the members of Parliament, CIS (Mar. 16, 2016)