



Aadhaar versus the right to privacy

Prashant

LL.M. Student, Directorate of Distance Education, Kurukshetra University, Kurukshetra, Haryana, India

Abstract

This Article attempts to highlight the impact of the Aadhaar on the right to Privacy which has been given under The Universal Declaration of Human Rights (UDHR), The International Covenant on Civil and Political Rights (ICCPR) recognize privacy as a fundamental human right. The Constitution of India does not expressly provide a right to privacy. However, the judiciary has read in the right to privacy within the ambit of existing Constitutional rights, specifically under right to life and personal liberty Article 21. This article is divided into three parts. Firstly, it traces the evolution of privacy laws in India. Secondly, it evaluates the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (“Aadhaar Act”), in light of privacy laws and constitutional validity. Finally, the article will weigh the potential data protection challenges of the Aadhaar scheme against the benefits of the system. In the absence of comprehensive data protection legislation, India’s tremendous Aadhaar scheme could pose considerable threat to the privacy of Indians.

Keywords: article universal declaration of human rights (UDHR)

Introduction

The Universal Declaration of Human Rights (UDHR) ^[1], The International Covenant on Civil and Political Rights (ICCPR) ^[2] and other international treaties ^[3] recognize privacy as a fundamental human right. Article 12 of the UDHR, Defines the Right to Privacy:

“no one shall be subject to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Meaning of Aadhaar

Aadhaar is a 12-digit unique identification number issued by the Indian government to every individual resident of India. The Unique Identification Authority of India (UIDAI), which functions under the Planning Commission of India, is responsible for managing Aadhaar numbers and Aadhaar identification cards.

The Aadhaar project was initiated as an attempt towards having a single, unique identification document or number that would capture all the details, including demographic and biometric information, of every resident Indian individual. Currently there are a plethora of identity documents in India including passports, permanent account numbers (PANs), driving licenses and ration cards. The Aadhaar card/UID will not replace these identification documents but can be used as the sole identification proof when applying for other things. It will also serve as the basis for Know Your Customer norms used by banks, financial institutions, telecom firms and other businesses that maintain customer profiles. Aadhaar numbers will eventually serve as the basis for a database with which disadvantaged Indian residents can access services that have been denied to them due to lack of identification documents ^[4].

Some countries, including India, do not expressly include the right to privacy in their Constitution. Despite a lack of legislation to this effect, the common law has developed a multi-faceted definition of the right to privacy. Over the past several decades, judicial activism in India has developed precedent wherein the right to privacy has been inferred through other articles of the Constitution. On July 19, 2017 a nine judge bench of the Supreme Court, led by Chief Justice Khehar, assembled to determine whether Indian citizens have a fundamental right to privacy under our Constitution.

In 2009, the Government of India constituted the Aadhaar scheme. This system, recognized as the world’s largest biometric identification scheme, provides national identification numbers for all residents. Critics of the Aadhaar scheme have highlighted several socio-economic issues. For the purpose of this article, the most significant concern surrounds the impact on privacy for Indians using the scheme. Without legislation defining the scope of the right to privacy, there are insufficient legal safeguards to control risks involving data collection and protection, which in today’s world has become absolutely crucial. It attacks the evolution of privacy laws in India through the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (“Aadhaar Act”). That’s why this article will attempt to weigh the potential data protection challenges of the Aadhaar scheme against the benefits of the system. In the absence of comprehensive data protection legislation, India’s tremendous Aadhaar scheme could pose considerable threat to the privacy of Indians ^[5].

Privacy Laws in India

The Constitution of India does not expressly provide a right to privacy. However, the judiciary has read in the right to privacy within the ambit of existing Constitutional rights,

specifically: freedom of speech and expression Article 19(1) (a)^[6] and right to life and personal liberty Article 21^[7].

Article 19(1) (a) stated that all the citizen shall have the right to freedom of speech and expression and article 21 of constitution of India stated that no person shall be deprived of his life or personal liberty except according to procedure established by law. The word life in article 21 means a life of dignity. In *Kharak Singh v State of U.P*^[8], the minority judgments of Subba Rao Hon'ble Judge and Shah Hon'ble Judge, held that the right of privacy does form an essential ingredient of personal liberty, as defined in Article 21. The majority, however, was of the alternate view that Article 21 could not be interpreted to include the right to privacy. This 1964 judgment was the first time the Supreme Court, albeit by a minority, explicitly recognized the existence of the right to privacy under Article 21. In the 1994 case of *R. Rajagopal v State of Tamil Nadu*^[9], the Supreme Court directly linked the right to privacy with Article 21 of the Constitution and held that, "the right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters. No one can publish anything concern the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages.

This position is reaffirmed in the 2012 judgment of *Ramila Maidan Incident*^[10], where the Supreme Court stated that "illegitimate intrusion into privacy of a person is not permissible as right to privacy is implicit in the right to life and liberty guaranteed under our Constitution." In 1970, benches of two and three-judges have expanded their reading of the ambit of the right to privacy. Despite these developments, the scope of the right to privacy is still limited rather than absolute. For instance, in 1975, in the case of *Gobind v. State of M.P*^[11] the Supreme Court stated "the right to privacy in any event will necessarily have to go through a process of case-by-case development. Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterize as a fundamental right. On the other hand the Information Technology Act (IT Act) 2000 also introduced the practice of reasonable security measures for preserving sensitive data of individual.

Privacy and the Aadhaar Scheme

i) Practical Challenges

Firstly, and most importantly, adequate legal safeguards must be implemented to protect the biometric information collected from individuals who have opted to participate in the Aadhaar scheme. It has been alleged that the data aggregation is sometimes conducted in a disorganized manner, resulting in various claims of information breaches. Personal data that is misappropriated during the collection stage will enable third parties to misuse confidential biometric and demographic information. Although the Aadhaar Act does restrict collection of information relating to race, caste, ethnicity, the data

collectors are still allowed to ask such questions. In a country as proudly diverse as ours, there should be strict prohibition on collection of such data.

Secondly, the collected data is stored in the Central Identities Data Repository. If this digitized database is compromised, the personal data of millions of individuals could be stolen. In fact, the Supreme Court, in its recent judgment *Binoy Viswam Vs Union of India*^[12] stated that: "it is also necessary to highlight that a large section of citizens feel concerned about possible data leak we emphasize that measures in this behalf are absolutely essential and it would be in the fitness of things that proper scheme in this behalf is devised at the earliest."

Aadhaar numbers are also used by defence and security personnel, any breach in the database would magnify the threat to national security interests. Finally, the Aadhaar Act in its current form does not provide for clear damages to the affected party, even where there has been a failure to protect personal data. India must amend these legislative provisions to develop.

1. Effective redressal mechanisms
2. Opportunities for judicial review of the same.
3. The financial and operational burden of managing such lawsuits must serve as encouragement for the Government to improve security in data collection and processing within the Aadhaar scheme.

ii) Constitutional Challenges

In 2009, the Government of India constituted the Unique Identification Authority of India ("UIDAI") to implement the Unique Identity ("UID") Scheme to collect UID data from Indian residents. The Aadhaar Scheme is governed by the Aadhaar Act. Through this legislation, the Government of India has: established the UIDAI; issued Aadhaar numbers to individuals; and maintained and updated information included in the Central Identities Data Repository. Additional objectives of the Aadhaar Act include: addressing issues pertaining to security, privacy and confidentiality of information, as well as clearly defining penalties for contravention of relevant statutory positions. While the UIDAI has maintained that the scheme is voluntary, the central government has pushed state governments to mandatorily link Aadhaar cards to a wide range of essential government services available to the public. In fact, to reduce public confusion, in the case of *K.S Puttaswamy (Retd.) v. Union of India and Ors*^[13], the Supreme Court passed an interim order that held: "the Aadhaar card scheme is purely voluntary and it cannot be made mandatory till the matter is finally decided by this court one way or the other." In conflict with this position is Section 139AA of ITA^[14]. Pursuant to the legislation, an Aadhaar number is mandatory for:

1. Obtaining a PAN
2. Continuing the validity of a person's PAN
3. Filing one's return of income under the ITA. The validity of Section 139AA of ITA has been challenged; arguably, this obligation is a violation of Article 14 and Article 19 (1) (g) of the Constitution. The Supreme Court passed a judgment on June 9, 2017 upholding the Government's position to link usage of the PAN and the Aadhaar card. However, the court further clarified that the PAN cards of non Aadhaar card holders who do not comply with

provisions of Section 139AA of ITA, should be treated as valid for the time being. Additionally, the validity of the said upheld provision is subject to the judgment of the Constitution Bench under Article 21 of the Constitution.

Conclusion

The Aadhar Act has deep-rooted issues attached to it when it comes to breach of security and ultimately privacy. There are other alternatives to implement Aadhaar which might make it a justified, clean and a clear programme. The Government's stance and defence in the matter is always focused towards the objective of evasion of corruption by implementing linkage of unique identification to PAN, Income Tax matters, banks, etc. to avoid crimes such as tax frauds. The Aadhaar scheme has more than lived up to its objectives. For example the Aadhaar scheme has greatly aided inclusive finance by adding more than 29 crores in new bank accounts, and saved the Government over Rs. 34000 crores through direct transfer of benefits (DBT). India must formulate stricter privacy control on the data collected. At present the Aadhaar regime has several unanswered privacy concerns that could result in an unfortunate and unnecessary setback to the whole regime. Therefore, the call for a comprehensive legislation for the protection of an individual's right to privacy is imperative, especially in light of the dramatic increase in the number of internet users in India every year. As in most cases, a judicious balance between protecting our fundamental rights and changing the lives and efficiencies of the majority of our citizens is the crux. Finally Government and judiciary will create a harmonious, win-win solution for all. However, the objective is of crucial importance, the privacy of citizens is of supreme importance as privacy is now a fundamental right in India.

References

1. Article 12 of the Universal Declaration of Human Right, 1948.
2. Article 17 of the International Covenant on Civil and Political Rights, 1966.
3. Article 7 and 8 of the Charter of Fundamental Rights of the European Union, 2012.
4. en.m.wikipedia.org.
5. Sflc.in.
6. Article 19(1) (a) of the Constitution of India.
7. Article 21 of the Constitution of India.
8. AIR 1963 SC 1295: 2 Cri LJ 329, 1963.
9. 1994 SCC (6) 632: 1995 AIR 264.
10. Re-Ramlila maidan Incident Dt v. Home Secretary and Ors 5 SCC 1, 2012.
11. 2 SCC 148: 1975 SCC (Cri) 468, 1975.
12. Writ Petition (Civil), 2017, 247.
13. Writ Petition (civil) no.494 of, Supreme Court of India, 2012.
14. Section 139AA, Income Tax Act, 1961.