INTERPLAY OF THE RIGHT TO PRIVACY VIS-À-VIS THE AADHAAR SCHEME

-Bahram N. Vakil[*]*, Saloni Bhandari*[**] *& Firoza Dodhi*[***]

I. INTRODUCTION

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

> "*no one shall be subjected 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.*"[2]

Yet, 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.[3] 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.

---

[*] Founder & Senior Partner at AZB Partners. LL.M, Columbia University; Member, NY State Bar Association.
[**] Associate, AZB & Partners. B.A.,LL.B (Hons.), Hidayatullah National Law University.
[***] LL.M candidate at University College London.
[1] D Banisar & S Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments,* 18(1) J. MARSHALL J. COMPUTER & INFO. L(1999).
[2] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N Doc. A/180 at 71 (1948).
[3] *Supra* note at 1.

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.

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 our view, in the absence of comprehensive data protection legislation, India's tremendous Aadhaar scheme could pose considerable threat to the privacy of Indians.

II. 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)] and right to life and personal liberty [Article 21].

In *Kharak Singh v State of Punjab*[4], the minority judgments of Subba Rao J. and Shah J., 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*[5], 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*

[4] Kharak Singh v. State of Punjab, (1964) 1 SCR 332.
[5] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

> *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, In re*[6] 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 fact, since the mid-1970's, 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*[7] 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, we do not think that the right is absolute."*

The decisions made at common law, demonstrate the Indian judiciary's vision to establish guidelines for the right to privacy. Even so, these definitions have focused extensively on personal privacy; there is a lack of judicial opinion regarding data privacy.[8] Given that India's outsourcing industry is a world leader, there is an immediate requirement for stronger data protection safeguards in the law. The Information Technology Act (**"IT Act"**) 2000 introduced the practice of reasonable security measures for preserving sensitive data.[9] In its current form however, the IT Act lacks sufficient provisions for the secure processing of personal data, or rules regarding data collection.

III. PRIVACY AND THE AADHAAR SCHEME

*(a)*PRACTICAL CHALLENGES

[6] In Re: Ramlila Maida Incident, (2012) 5 SCC 1.
[7] Gobind v. State of M.P, (1975) 2 SCC 148.
[8] Subhajit Basu, *Policy Making, Technology and Privacy in India,* 6 IND. J. OF L. & TECH. 65, 69-74(2010).
[9] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

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.[10] 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[11] 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.*"

Perhaps more significantly, as 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.[12] India must amend these legislative provisions to develop: (i) effective redressal mechanisms and (ii) opportunities for judicial review of the same. 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.

(b) 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

[10] G. Greenleaf, *India's National ID System: Danger grows in a Privacy Vacuum,* 26 COMPUTER LAW AND SECURITY REVIEW 479-491 (2010).
[11] Binoy Viswam v. Union of India, 2017 (6) SCALE 621.
[12] *Id.*

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.[13]

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 v Union of India*[14], 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 the Income Tax Act ("**ITA**"). Pursuant to the legislation, an Aadhaar number is mandatory for: (i) obtaining a PAN; (ii) continuing the validity of a person's PAN; and (iii) 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.

IV. CONCLUSION

The Aadhaar scheme has more than lived up to its objectives. Just by way of 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). However, as the Aadhaar scheme covers 1.1 billion Indians (by far, the world's largest and most sophisticated ID scheme), India must formulate stricter privacy control on the data collected. At present the Aadhaar regime has several

[13] Statement of Objects and Reasons, Aadhaar Act.
[14] K.S Puttaswamy v. Union of India, (2015) 10 SCC 92.

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. We are cautiously optimistic that the Government and judiciary will create a harmonious, win-win solution for all.