RIGHT TO PRIVACY IN INDIA: VIS-À-VIS AADHAR SCHEME

Written by ***Ashish Sancheti***

3rd Year BBA LL.B (Hons.) Student, School of Law, Christ University, Bangalore

ABSTRACT

Any Information holds a value and is a property, but, privacy is not a property since it's of autonomous domain. A complete denial of privacy will defeat democracy, but so will an absolute right to privacy. The Supreme Court of India has upheld privacy as a fundamental right under Article 21 and part III of the Constitution. This means privacy will have no definition - its scope and definition will be decided on a case to case basis. Despite the right to privacy being accorded judicial recognition time and again, there still does not exist a cogent legal framework for privacy laws in India. There exists in India an alarming need to enact a law with a view to safeguard the Right to privacy of an individual. The need for such a statute becomes more desirable when one notices that there are no existing regulations which can safeguard personal information disclosed by an individual. Unless a concrete legislation on this subject addresses ground reality, the right to privacy will remain a right on paper. The restrictions on the privacy will depend upon which article it emanates from. The aim of this paper is to ponder the issues relating to Right to Privacy under the Aadhaar Scheme. At the end, the article proposes suggestions in order to fulfil the need of privacy laws in the country.

Keywords: Privacy, Aadhaar, Right to privacy, Personal Information

INTRODUCTION – CONCEPT OF PRIVACY

The concept of Right to Privacy paved its way through a seminal piece published in the Harvard Law Review [1]in 1890. Warren and Brandeis argued that it was necessary for the legal system to recognize the right to privacy because, when information about an individual's private life is made available to others, it tends to influence and even to injure the very core of an individual's personality-"his estimate of himself."[2] However, it was Brennan J who developed this right in its fullness in *New York Times Co. V. Sullivan*,[3] followed and applied in *Time V. Hill* [4]

A concern that the opposition to the right to privacy immediately raises, is how we define "privacy" and the scope of application of a "right to privacy a good approach through which privacy can be defined is to strike a balance between the reductionist and the antireductionist attempts at defining privacy.[5] The reductionist philosophy would state that the ambit of privacy and its violation should be specified by the legislature.[6]

Privacy has been traditionally considered as a right in evolved legal jurisdictions. However, the growth of human rights jurisprudence across the board in municipal as well as international law, has led to the elevation of privacy as a significant area for right based law. Most public and consumer services today depend on transactions based on data that is often sensitive and personal in nature. In other words, a person today is required to reveal a lot more about his private life in order to receive services that are mostly essential. The right to privacy has conventionally been enforced in courts of law by subjective considerations depending on the circumstances of each claim. The scope and extent of privacy as a social construct varies across

[1] Warren and Brandeis, '*The right to privacy'*, 4 Harvard Law Review 193, (1890).
[2] Dorothy J. Glancy, '*The invention of the right to privacy'*, 21 Arizona Law Review 1, 2(1979).
[3] II L Ed 2d 686: 376 US 254 (1964).
[4] 17 L Ed 2d 456: 385 US 374 (1967).
[5] Ujwala Uppaluri & Varsha Shivanagowda, '*Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating toward a Privacy Right in India'*, 5 NUJS L. REV. 21 (2012).
[6] Madison Powers, '*A Cognitive Access Definition of Privacy'*, 15 LAW & PHILO. 369 (1996).

societies. In most jurisdictions courts seek to employ subjective standards of privacy with reference to the facts of a particular case.

INDIAN CONSTITUTIONAL AND LEGAL PERSPECTIVE ON PRIVACY AND DATA PROTECTION

In the period before the coming of the present constitution, no rights were accorded to citizens. The legal concept of citizenship and enforceable rights in India came into being with the Constitution of 1950. Privacy has been a cherished value in human rights law across jurisdictions. Privacy was not specifically enumerated in the bill of rights in India. However, it has been incorporated in the constitution under the aegis of Article 21 by virtue of various pronouncements of law by the Supreme Court. Therefore, in public law, privacy is a fundamental right. Its breach is to be remedied by the constitutional courts under the writ jurisdiction.

Zonal form of privacy

The Zonal form of privacy was first recognised in the Third and Fourth Amendments to the United Stated Constitution. While the Third Amendment [7] stated that "No soldier shall, in time of peace be [quartered in any house], without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law"; the Fourth Amendment[8] upheld the "The right of the people to be [secure in their persons, houses, papers, and effects] against unreasonable searches and seizures shall not be violated". The zonal paradigm was also addressed by Justice Harry Blackmun, when he concluded in his dissent[9] that "the right of an individual to conduct intimate relationships in the intimacy of his or her own home seems to me to be the heart of the

[7] U.S. CONST., amend III.
[8] U.S. CONST., amend IV.
[9] *Bowers v. Hardwick*, 478 U.S. 186 (1986) (Blackmun J. dissenting).

Constitution's protection of privacy." This was also tacitly recognised by the Supreme Court of India in *Gobind v. State of Madhya Pradesh*, where it noted that "any right to privacy must encompass and protect the [personal intimacies of the home], the family marriage, motherhood, procreation and child rearing."[10] Similarly, the Supreme Court of India in *Suresh Kumar Koushal v. NAZ Foundation*[11] held that any activity criminalized by the IPC cannot be protected under the right to privacy, even if it occurs with the personal intimacies of home. The Supreme Court in its *Gobind*[12] decision noted that privacy-dignity claims can only be denied when a superior countervailing State interest is present.

Interpretation of term 'Privacy' by Apex Court

The question of a constitutional right to privacy under Part III of the Constitution was first raised in the decision of *Kharak Singh v. The State of UP* [13]where the petitioner was subjected to continuous surveillance as under Regulation 236 of the U.P. Police Regulations. Although, the Supreme Court began to accept certain points of the minority view[14], the right to privacy was still waiting for its place in Indian constitutional jurisprudence.[15] In *Gobind v. State of Madhya Pradesh* [16]the Supreme Court held that a "limited" right to privacy was implied within the ambit of Part III of the Constitution, which originates from the Articles 19(a), 19(d) and 21.

The Supreme Court of India has time and again upheld the decisional right to privacy of individuals, and has even gone to the extent of upholding an individual's decision to take

[10] *Gobind v. State of Madhya Pradesh*, 1975 SCR (3) 946.
[11] AIR 2014 SC 563.
[12] AIR 1975 SC 1378.
[13] AIR 1963 SC 1295.
[14] *State of West Bengal v. Ashok Dey*, AIR 1972 SC 1660; *Haradhan Saha v. State of West Bengal*, AIR 1974 SC 2154; *John Martin v. State of West Bengal*, AIR 1975 SC 77.
[15] Jain, M.P., The Supreme Court and Fundamental Rights in S. K. VERMA, KUSUM (EDS.), FIFTY YEARS OF THE SUPREME COURT (Oxford University Press 2015).
[16] AIR 1975 SC 1378.

vegetarian or non-vegetarian food as a paramount personal affair protected under the right to privacy. [17]

In 1954, the Supreme Court in *M. P. Sharma v. Satish Chandra*[18], rejected the contention that there exists a right to privacy under Article 20(3)[19]due to the absence of any provision analogous to the Fourth Amendment of the US Constitution. It was the first claim for a right to privacy, the court speaking through a three judge bench held:

> "*When the constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the [American] Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction*."

The Supreme Court in *Sunil Batra v. Delhi Admn* [20]observed that a minimal infringement of a prisoner's privacy is unavoidable as the officers have an obligation to keep a watch and ensure that their other human rights are being duly observed. The Court in *Malak Singh v. State of P&H*[21] held that surveillance is a direct encroachment upon an individual's right to privacy. In *Selvi v. State of Karnataka*[22] it was held that any techniques that interfere with a person's mental processes in order to extract information are an infringement of right to privacy.

In *R. Rajagopal v. State of Tamil Nadu*[23] it was again asserted that the right to privacy is an implicit right under Art. 21[24] and has acquired sufficient constitutional status. The Court noted that the said right includes a "right to be let alone" and the right "to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among

[17] *Hinsa Virodhak Sangh v. Mirzapur Mot Kureshi Jamaat*, AIR 2008 SC 1892.
[18] AIR 1954 AIR 300.
[19] INDIA CONST. Art. 20(3).
[20] (1978) 4 SCC 494.
[21] AIR 1991 SC 760.
[22] (2010) 7 SCC 263.
[23] AIR 1995 SC 264.
[24] INDIA CONST. Art. 21.

other matters". [25] It was in this case that the scope and ambit of the right to privacy or the right to be left alone came up for consideration before the Supreme Court. The court placed reliance on the seminal article by *Warren and Brandeis*[26] which defined the concept of the right to be left alone. The Supreme Court recognized the need to limit the scope of privacy so as to prevent it from impacting transparency and legitimate freedom of expression. Therefore, comments made on matters in the public records are precluded from claims of privacy claims both in private and public law.

On a similar note, in *State of Maharashtra v. Madhukar Narayan Mardikar* [27] the Supreme Court held that even a "woman of easy virtue" is entitled to her privacy and nobody has the authority to invade her privacy at their sweet will.[28] The Supreme Court in *S.P. Gupta v. President of India*[29] held that a balance needs to be struck between the right to information and right to privacy. The Supreme Court in *Suresh Kumar Koushal v. NAZ Foundation* [30]held that Section 377 of the Indian Penal Code, criminalising any form of "carnal intercourse", does not suffer from any vice of unconstitutionality. Moreover, elaborating on the relational aspect of privacy, the Supreme Court in *Directorate of Revenue v. Mohd. Nisar Holia*[31], held that "right to privacy deals with persons and not places".

In *Bharat Shanti Lal Shah*[32] case, the court held that a statute can authorise the interception between two individuals even when it is a direct violation of their right to privacy, if the procedure authorizing such violation is just, fair and reasonable and not arbitrary or oppressive. It has been noted that any act claimed under the relational form of privacy should be-firstly, principally and fundamentally private and intimate in nature and secondly, in accordance with

[25] *R. Rajagopal v. State of Tamil Nadu*, AIR 1995 SC 264.
[26] Louis D. Brandies and Samuel Warren, *"Introduction" in the Right to Privacy*.
[27] AIR 1991 SC 207.
[28] *Indian Drugs and Pharmaceuticals Ltd v. Workmen*, (2007) 1 SCC 408.
[29] AIR 1982 SC 149.
[30] AIR 2014 SC 563.
[31] AIR 2009 SC 1032.
[32] *State of Maharashtra v. Bharat Shanti Lal Shah*, (2008) 13 SCC 5.

the law of the land.[33] In *Ram Jethmalani v. Union of India*[34], the Supreme Court has held that right to privacy is an integral part of life. This is a cherished constitutional value and it is important that human beings be allowed privacy, and is free of public scrutiny unless they act in an unlawful manner.

The 'Aadhaar' Case

Complaints about the Aadhaar system made to India's High Court focused on privacy voluntariness.[35] The Supreme Court in *Justice K.S. Puttaswamy v. Union of India*[36] known famously as the *Aadhaar Card* decision has opened the debate wide on whether privacy is a fundamental right. Justice Bobde and Justice Chelameshwar have expressed concern over Aadhaar forcing people to registration are not able to comprehend the consequences of registration on their rights. Justice Bobde has also expressed concerns over the already happened and future leaks of information concerned. The Supreme Court decided that Indians have fundamental right to privacy; the next big question is whether the *Aadhaar Act* will be struck down for violating that right. Justice (Retd.) Puttaswamy (Petitioner) challenged the Aadhar Card Scheme on various grounds. One of his main contentions is that the collection of biometric data of the said scheme violates the "right to privacy". At the time of application of the Aadhaar Card, an applicant has to provide his biometric data. The Petitioner stated that this is a violation of Article 21 of the Constitution of India, 1950, which grants "right to Privacy" as a fundamental right through various decisions of the Apex Court.

Mr. Mukul Rohatgi, Attorney General of India, who appeared on behalf of one respondent, before the three judge Bench of the Hon'ble Supreme Court brought two case laws on the subject to the attention of the Court; *M.P. Sharma & Ors. v. Satish Chandra & Ors* and *Kharak*

[33] Abhinav Chandrachud, '*The Substantive Right to Privacy: Tracing the Doctrinal Shadows of the Indian Constitution'*, (2006) 3 S.C.C. (Jour.) 31.
[34] (2011) 8 SCC 1.
[35] Supreme Court of India, Writ Petition (Civil) No. 494 of 2012.
[36] (2014) 6 SCC 433.

Singh v. State of U.P. & Ors, an eight and six judge Bench decision of the Court, respectively. In both these cases, the Hon'ble Supreme Court has been doubtful about the position of "right to privacy" as a fundamental right.

Further, Mr. K.K. Venugopal, appearing on behalf of another Respondent, pointed out that the decisions of the apex court relied upon by the Petitioner have been made by a bench of two or three judges. Thus, due to this divergence in opinion, the Attorney General and Mr. Venugopal requested the Hon'ble Court to settle the legal position of the matter by placing it to be heard before a larger Bench of the Hon'ble Supreme Court. The Supreme Court recognized that the present case raises questions of far reaching importance involving interpretation of the Constitution of the precious and inalienable right to liberty under Article 21. In its interim order dated 11th August, 2015, the Court was of the opinion that keeping in view the possibility of commercial exploitation of biometric information of individuals and at the same time considering the benefits ensured by the Aadhaar Scheme in several social benefit schemes of the Government like MGNREGA, PDS system and distribution of LPG, restraining the respondents in issuing further Aadhaar cards will not be necessary. The Court said that the balance of interest will be best served by a larger bench; however UIDAI was directed not to use the information obtained for any other purpose, except as may be directed by a court for the purpose of criminal investigation.

In the case *PUCL v. Union of India*[37], with respect to the wiretapping of politician's phone calls to be considered as unconstitutional, it was held that the right to privacy has not been itself identified under the constitution. As a concept it may be too broad and moralistic to define it judicially .Whether the right to privacy can be claimed as or has infringed in a given case would depend upon the facts of the given case. However the court went on to hold that the "*the right to hold a telephone conversation in the privacy of one's home or office without any interference can be claimed as right to privacy."* From Article 19 Right to privacy can be derived as follows

[37] AIR (1997) SC 568.

"*When a person is talking on telephone, he is exercising his freedom of speech and expression*", the court observed and therefore "*telephone-tapping unless it comes within the grounds of restriction under article 19(2) would infract article 19(a) of the constitution".* In this way, it can be inferred that there has been a quiet accord among the judiciary to reach at a position where right to privacy stands a strong ground in the constitution. 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.[38] The US Supreme Court in *Planned Parenthood v. Casey*[39] provided its most elaborate explanation on the relation between "privacy" and "personal liberty. It stated that matters involving the most intimate and personal choices which are central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment and thus, should be protected. In 2002, the National Commission to Review the Working of the Constitution [40] recommended a constitutional amendment in the form of Article 21-B[41], which shall make "right to privacy" a fundamental right under Part III of the Constitution. Moreover, there was also a proposed Privacy Bill in the legislature during the year 2011. The bill was drafted with the objective of creating a statutory Right to Privacy, but is yet to be adopted by the Parliament.

[38] Subhajit Basu, '*Policy Making, Technology and Privacy in India'*, 6 IND. J. OF L. & TECH. 65, 69-74(2010).
[39] 505 U.S. 833 (1992).
[40] Ministry of Law & Justice, Government of India, Report on National Commission to Review the working of the Constitution, Report 62 (2002).
[41] "Art. 21-B. - (1) Every person has a right to respect his private and family life, his home and his correspondence. (2) Nothing in clause (1) shall prevent the State from making any law imposing reasonable restrictions on the exercise of the right conferred by clause (1), in the interests of security of the State, public safety or for the prevention of disorder or crime, or for the protection of health or morals, or for the protection of the rights and freedoms of others."

Data Protection in India

Data protection principles are designed to protect the personal information of individuals by restricting how such information can be collected, used and disclosed.[42] The protection of privacy permits individuals to plan and carry out their lives without unnecessary intrusion.[43] Informational privacy is often understood as the freedom of individuals *"to determine for themselves when, how, and to what extent information about them is communicated to others".*[44] In the present scenario citizens avail of a variety of services from government and private organizations. These transactions involve the furnishing of large amounts of data that is usually comprised of sensitive or personal information. This information is often required for the provision of the service sought to be availed, however, there may be cases wherein such data is collected for collateral purposes. Therefore, the *Information Technology (Amendment) Act, 2008 (ITAA)* introduced *Section 43-A* with the purport of creating privacy protection for information held by private intermediaries. It seeks to prevent unauthorized disclosure of *"Sensitive personal data or information".*

Data protection in India is governed by loosely constructed provisions of the ITAA under Sections 43-A and 72A of the Act. There is no definition available in the main statute for sensitive personal data or information or personal information. The third explanation appended to the section provides for the Central government to define the same in consultation with professional bodies. Pursuant to this the government enacted the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (hereinafter referred to as *Personal Data Rules*.) Personal information under the said rule is such information that can be used in one form or another to identify a natural person.

[42] Lee Bygrave, '*Data Protection Law: Approaching Its Rationale, Logic, and Limits'* 2 (Kluwer Law International: The Hague/London/New York, 2002).
[43] *Time, Inc. v. Hill*, 385 U.S. 374, 413 (1967) (Fortas, J., dissenting); *Doe v. Bolton*, 410 U.S. 179, 213 (1973) (Douglas, J., concurring).
[44] Alan Westin, 'Privacy and Freedom', 7, (Atheneum, 1967).

Further, the Personal Data Rules creates a classification of information under sensitive personal data. Section 43-A does not specifically define the nature and extent of security practices. The Central government is empowered to establish such standards arguably to maintain dynamism of the law with respect to changing technology. The Personal Data Rules were formulated to establish such standards and practices and at present is the most comprehensive form of data protection prescribing protocols and procedures. However, the Act fails to define *"sensitive data"* and states the same as *"personal information as may be prescribed by the Central government."*[45] It is to be noticed that Clause 30 of IT Act, 2000 states that biometric or demographic data are recognized as an *'electronic and sensitive data of an individual'*, and if someone tries to steal it, there is a Clause 34-47 under Chapter VII of IT Act, 2000 which deals with punishment related to it, and also is entitled as 'Offences and Penalties.'[46]

Data and information is an important part of everyday life in today's world. Most transactions are carried out by employing large amounts of information that may include addresses, financial details, and health records among others. This necessitates the formation of large public databases that will aggregate large amounts of data which would include data from every facet of a person's life. Therefore, the need to devise a privacy and data protection regime that would secure privacy rights of citizens across the country is obvious. The conception of privacy under the IT Act, 2000 is fairly limited in view of the position take in jurisprudence across jurisdictions. The protection regime lacks robustness. The dynamic nature of technology and its use across the board gives rise to a new facet of privacy protection. The requirement for a comprehensive law on data protection that encompasses government and private agencies remains unfulfilled.

[45] *Ibid*.
[46] Greenleaf G. Confusion as Indian Supreme Court Compromises on Data Privacy and ID Number. 137th edn. Privacy Laws & Business International Report, 2015.

INDIAN LEGAL FRAMEWORK ON AADHAAR

In recent years, governments have acted to build pervasive digital identity ecosystems.[47] A fingerprint is probably the best known biometric; fingerprints have been used in ink-and-paper forms for law enforcement purposes for decades, for example, the US government began maintaining a database of fingerprints in 1904.[48]

Aadhaar Act

The Aadhaar Act enables the Government to collect identity information from citizens[49] including their biometrics, issue a unique identification number or an Aadhaar Number on the basis of such biometric information[50], and thereafter provide targeted delivery of subsidies, benefits and services to them.[51] The Aadhaar Act is now the current statutory backing for the Aadhaar identification system.[52] The Aadhaar Act was updated in September, 2016 with regulations, which expanded the power of the Unique Identification Authority of India (UIDAI) and gave the government of India substantial ability to access the Aadhaar data, with broad abilities to use the data for law enforcement purposes.[53] *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour*

[47] World Bank Open Data. Identification for development global dataset, January 2016. **Available at: http://data.worldbank.org/data-catalog/id4d-dataset.** (Last visited on 30.06.18).
[48] Barnes page 16: "On October 19, 1904, Inspector Ferrier and Major M. W. McClaughry began fingerprinting all inmates at the Leavenworth, KS, federal prison. These fingerprint records became the beginning of the U.S. Government's fingerprint collection."
[49] Section 30, Aadhaar Act.
[50] Section 3, Aadhaar Act.
[51] Section 7, Aadhaar Act.
[52] Economic Times, Budget 2016: *'Full text of Finance Minister Arun Jaitley's speech regarding The Aadhaar Act,'* March 1, 2016. **Available at: https://economictimes.indiatimes.com/news/economy/policy/budget-2016-full-text-of-finance-minister-arun-jaitleys-speech/articleshow/51194097.cms** (Last visited on 2.07.18).
[53] Unique Identification Authority of India Regulation, 2016, No. 13012/64/2016/Legal/UIDAI (No. 1 of 2016.) the (Targeted Delivery of Financial and Other Subsidies, Benefits and Services), The Gazette of India, Sept. 12, 2016, **Available at: https://github.com/cis-india/uidai-docs/blob/master/UIDAI/Act%20and%20Rules/The-Gazette-of-India_Unique-Identification-Authority-of-India-Regulations-2016_20160914.pdf** (Last visited on 2.07.18).

and reputation. Everyone has the right to the protection of the law against such interference or attacks."[54] *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondence, nor to unlawful attacks on his honour and reputation".*[55] 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.[56]

Role of Unique identification authority of India

Unique Identification Authority of India (UIDAI) is a governmental agency of New Delhi that serves as an issuing authority of unique identity card (UID) and number's, The UID provides a unique identity to an individual by obtaining his private information in the form of finger prints and vision pattern. The card and the identification number on it are the proof of the identity and address of the individual. So the basic question which arises here is that how UIDAI affects the Right to Privacy of an individual. The Aadhaar Security Regulations impose an obligation on the UIDAI to have a security policy which sets out the technical and organizational measures which will be adopted by it to keep information secure.[57] The process of verification and application for the Aadhaar Card involves biometric data capture which includes capturing a digital print of facial image, the iris of the applicant and fingerprints. The UIDAI allots a unique identifier (Aadhaar Number) to each citizen and deposits their biometric and demographic data in a *Central Identities Data Repository* (CIDR).[58] UIDAI has also not mentioned clearly the use of the Aadhar card except mentioning that it has many uses such as it can be used as identity proof and seeks to be a gateway to the services, being

[54] Article 12, Universal Declaration of Human Rights (UDHR), 1948.
[55] Article 17, International Convention on Civil & Political Rights (ICCPR).
[56] Statement of Objects and Reasons, Aadhaar Act.
[57] Regulation 3, Aadhaar Security Regulations.
[58] Unique Identification Authority of India, DDSVP Committee Report, Planning Commission, December 09, 2009, **Available at: https://uidai.gov.in/images/UID_DDSVP_Committee_Report_v1.0.pdf** (Last visited on 28.6.18).

sufficient to know your customers' details in various things like opening a bank account or getting mobile numbers or for various other government services. A significant majority of India's residents now have the Aadhaar ID; as of 2016, 97% of adult Indians, and 67% of children are enrolled.[59]

The government of India has been linking the Aadhaar card with various government schemes such as for cooking gas subsidies, house allotments, school scholarships, admission into remand and welfare houses, passports, e-lockers for archiving documents, bank accounts under PMJDY (**P**randhan **M**antri **J**an **D**han **Y**ojana), provident funds account, pensions, driving license, insurance policies, loan waivers and many more.[60]Enrollment under the Aadhaar scheme is optional but there have been several incidents whereby people have been deprived of their benefits, reason being they weren't enrolled under the Aadhaar scheme.[61]

The biometric information so provided are important from the government's perspective and there lies a number of advantages like Aadhar based Direct Transfer Subsidy, Jan Dhan Yojna , Passport in 10 days, Digital locker, Voter Card Linking, Monthly Pension Provident Fund Opening new bank account, Digital Life Certificate and SEBI facilities. Although the Aadhaar Act does restrict collection of information relating to race, caste, ethnicity, the data collectors are still allowed to ask such questions.[62] 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.[63]The Supreme Court passed an ad-interim order in *Unique Identification Auth. of India*

---

[59] Parliamentary Debate, Aadhaar Act, 2016, p. 329. **Available at: http://164.100.47.132/newdebate/16/7/11032016/12To1pm.pdf** (Last visited on 1.07.18).
[60] Sen. KM. *'Aadhaar: Wrong Number, Or Big Brother Calling.' Socio-Legal Rev.* 2015, 11 (2), pp. 85-108.
[61] Mandhani Apoorva,*"Meanwhile, the Petitioners shared affidavits of instances where citizens had been denied their rights: among them, an instance of a non-processing of a scholarship for a poor person, another of an individual denied a voters identity card for the lack of an Aadhaar card, and another of bank accounts not being allowed without Aadhaar."*- SC reserves order on transfer of Aadhaar Challenge to Const. Bench; AG says Privacy not a Fundamental Right, *Livelaw.in,* August 6, 2015 (last visited on 1.7.2018).
[62] G. Greenleaf, '*India's National ID System: Danger grows in a Privacy Vacuum',* 26 COMPUTER LAW AND SECURITY REVIEW 479-491(2010).
[63] *Binoy Viswam v. Union of India*, 2017 (6) SCALE 621.

and anr. v. *Central Bureau of Investigation*[64]where it held that the Unique Identification Authority of India was restrained from transferring anyone's biometric information with an Aadhaar number to any other agency without such person's consent in writing.

The National identification authority bill, 2010

The National Identification Authority Bill, 2010 under Section 33 (b) empowers the government to access data in the CIDR which constitutes the National Population Register. It's a clear case of State's intrusion of the citizen's privacy. The State, under the guise of security and national interest, is putting law abiding citizens under surveillance, restricting their freedoms and infringing their right to privacy. Hon'ble court in *M.P. Sharma's case* had no justification to acknowledge right to privacy as protected under Article 21, it restricted itself only to Article 20(3) of the Constitution.[65] In this scheme an individual has to submit his biometric data and his iris and fingerprints are scanned but there is no proper system in place to safeguard that all this data and prevent misuse. This scheme is not supported by a legislative authorization and is still in force only as an administrative notification.[66] In *Shantistar v. Narayan*[67], the Hon'ble Court stated that Article 21 comprised of rights with regard to a member of the weaker sections of the society, and they would be provided with residential housing, including pavement inhabitants.[68] So, if an individual is deprived of any benefit under a welfare scheme on the reason of him not having an Aadhaar card, to which he would have been otherwise eligible to, then such a declination is an infringement to his right to life. Bearing in mind the wide spread infringement of its previous orders, the Court in August 2015 issued a number of instructions. It ordered the Centre to give wide promotion through electronic and print media that the card is not compulsory to be eligible for the government schemes.

[64] Petition(s) for Special Leave to Appeal (Crl) No(s).2524/2014 in the Supreme Court, Order dated March 24, 2014.
[65] Article 20(3) - No person accused of any offence shall be compelled to be a witness against himself.
[66] Notification No.-A-43011/02/2009-Admn.I, 28 January 2009, Planning Commission, Government of India" (PDF). UIDAI, January 28, 2009 (last visited on 1/7/18).
[67] (1990) 2 SCJ 10.
[68] *Sodan v. N.D.M.C,* (1990) 3 SCJ 431.

Furthermore, it was asserted that *"Aadhaar will not be used for any other function except Public Distribution System (PDS), kerosene and LPG distribution system."* However, the Court asserted the fact that even for availing benefits under PDS, kerosene and LPG distribution system, the card shall not be made compulsory.

Biometrics and UIDAI

In one of the articles, Justice P.S Puttaswamy, retired judge of Karnataka High court said, *"There are no safeguards or penalties and no legislative backing for obtaining personal information, and the proposed law introduced by the government has been rejected by the Parliamentary Standing Committee on Finance. Provisions for collection and retention of biometric data have been held impermissible in the United Kingdom and France by their top courts."*[69] A trade-off between the Aadhaar and Right to privacy is incomprehensible. Our evolving constitutional jurisprudence on privacy rights post *M.P Sharma & Ors. v. Satish Chandra, District Magistrate Delhi & Ors*[70], unambiguously affirms the right to privacy as an integral part of the right to life and right to personal liberty envisaged in the expansive interpretation of Article 21.

The biometric is not an absolutely accurate standard and there is a likelihood of error.[71] The National Identification Authority of India Bill, 2010 sought to allow the use of Aadhar data for the purposes of national security without the consent of the person whose data is being shared.[72] But the constitutional validity of this bill if it becomes a law remains to be tested against the established standards of the law against self-incrimination and the standards of

[69] J.Venkatesan, *Aadhar Infringes Privacy*, THE HINDU, Sep 23, 2013.
[70] (1954)AIR 300.
[71] Alan Gelb and Julia Clark, Performance Lessons from India's Universal Identification Program, CGP Policy Paper 2013, **Available at http://www.cgdev.org/sites/default/files/biometric-performance-lessons-India.pdf** (Last visited on 8.07.18).
[72] Section 33: Nothing contained in sub-section (3) of section 30 shall apply in respect of—
… any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer or officers not below the rank of Joint Secretary or equivalent in the Central Government specifically authorized in this behalf by an order of the Central Government.

privacy in India.[73] From time to time Supreme Court has recognized right to privacy as a fundamental right no matter on what grounds the centre has denied it as a fundamental right. The constitutional jurisprudence has also recognized the right to privacy as an ultimate right to protect individual's private or personal life. UIDAI is definitely violative of the fundamental right of privacy as it misuses the personal information for a variety of purposes not only by government organization but also private institutions. The cure which the government has to look for to solve this problem is to completely abolish this biometrics information providing system in UIDAI as it will not lead to any security or privacy issue. The finger prints or the retina scan or any other biometric method of storing one's personal information and then using it without his consent is totally violative of the fundamental right of right to privacy envisaged in right to life under article 21 forming the heart of fundamental rights. With the above mentioned facets of right to privacy and how unique identity affects the right to privacy provided to us by Indian constitution the author concludes that as far as biometric information is concerned in the UDI it is infringing the right to privacy of the individuals and would cause serious issues with individuals as well as national security.

DATA PROTECTION AND PRIVACY LAWS IN U.K.

Human rights in the UK are rooted in common law. The history of human right protection in English law can be traced to the Bill of Rights, 1689. Personal information is deemed to be sensitive and particularly vulnerable to unauthorized access, use, modification and disclosure thereby requiring safeguards and appropriate security. The aspect of sensitivity is manifestly contained in the personal information collected from data subjects. The Organization for Economic Cooperation and Development (OECD) privacy principles also focus on the reinforcement of limitations on data use and disclosure by security safeguards. It enlists

[73] *Kharak Singh v. The State of U.P. & Ors.* (1964) 1 SCR 332; *People's Union of Civil Liberties v the Union of India* (1997) 1 SCC 318; *State of Bombay v. Kathu*, AIR1961 S.C.1808.

physical measures such as identification cards, organizational measures such as authority levels with regard to access to data and informational measures such as enciphering and threat monitoring of unusual activities and responses to them. International organizations, such as United Nations[74], the OECD[75], the Council of Europe and the European Community (EC), have invested heavily in data protection, issuing guidance and laws that are remarkably consistent in terms of their aims, objectives and requirements.

European Convention on Human Rights

In the wake of popular opinion, the British Parliament enacted the Human Rights Act, 1998 in order to implement the European Convention on Human Rights (ECHR). The enactment of the Human Rights Act, 1998 lent statutory force to various rights provided in the ECHR including the right to privacy. Article 8 of the ECHR protects the right to privacy and provides the founding principles upon which European data protection laws are built.[76] It is important to recognize that the connection between the ECHR and European data protection laws is inviolable. Data protection laws are best regarded as modified privacy laws, in the sense that they build upon the right to respect for privacy contained in Article 8 of the ECHR, in order to provide clearer protections for the privacy of personal data undergoing processing. If data protection laws are viewed in their wider context it will be seen that despite the limitation they place on the protections for the manual processing of personal data, privacy in manual data is generally protected due to the right to privacy within Article 8 of the ECHR. In the UK a breach of confidence action can be used to protect the right to privacy if in the circumstances of the case the data subject has a reasonable exception of privacy. UK laws have moved on

[74] Guidelines for the regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990.
[75] Recommendation of the council of the OECD concerning Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data, 23 September 1990.
[76] Stewart Room, *Data protection and compliance in context*, BCS, The Chartered Institute for IT; 1 edition (November 27, 2006), p.5.

significantly since the introduction of the Human Rights Act and clarification of the fact that the protections in Article 8 of the ECHR extend to threats from the private sector.[77]

Biometric systems provide a valuable service in helping to identify individuals from their stored personal details. Unfortunately, with the rapidly increasing use of such systems[78] there is a growing concern about the possible misuse of that information. In 2006, for example, a telephone survey by the UK Information Commissioner's Office revealed that over 45% of respondents viewed biometric data as 'extremely sensitive'[79] There are also psychological objections to biometric use, with some suggesting that measurements of a person's body are inherently more personal than other data about them.[80]

By late May of 2018, anyone doing business within the EU's 28 member nations will need to abide by new mandates and limitations imposed by the GDPR.[81] The EU, through the new data protection regulations articulated in the GDPR, has sought to exercise greater control over data protection and privacy matters than the existing Data Protection Directive, EU 95/46.[82] The processing of sensitive data,[83] which in the GDPR for the first time includes biometrics

[77] Stewart Room, *Data protection and compliance in context*, BCS, The Chartered Institute for IT; 1 edition (November 27, 2006), p.7.
[78] Article 29 data protection working party, "Opinion 03/2012 on developments in biometric technologies," April 2012.
[79] K. McCullagh, "*Data Sensitivity: Proposals for Resolving the Conundrum*" Journal of International Commercial Law and Technology, Vol. 2, Issue 4, 2007.
[80] J. D. Woodward, K. W. Webb, E. M. Newton, M. A. Bradley, D. Rubenson, K. Larson, J. Lilly, K. Smythe, B. Houghton, H. A. Pincus, J. Schachter, P. S. Steinberg, "*Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*" Rand Corporation.
[81] EU General Data Protection Regulation, (EU-GDPR). **Available at: http://www.privacy-regulation.eu/en/index.htm** (Last visited on 6.07.18).
[82] EU/95/46/EC, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[83] Sensitive data in the EU-GDPR is defined in Article 9 of the GDPR. "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." EU General Data Protection Regulation, (EU-GDPR), Article 9 "Processing of special categories of personal data."

specifically, generally requires "explicit" consent. For a data controller to demonstrate explicit consent, they must meet robust requirements.[84]

Data Protection Act

In the UK the framework piece of legislation is the Data Protection Act, 1998, (DPA). The DPA repealed and replaced its predecessor, the Data Protection Act, 1984 in order to give effect to the requirements of the EC Data Protection Directive, 1995. The data protection registrar so created by the 1984 Act was also replaced in 1998 by the data protection commission.[85] The DPA also gives effect to the requirements of the Council of Europe's Data Protection Convention, 1981.

Before understanding the intricacies of the act, we must first understand the concept of 'Data subject', 'Data controller', 'Data processor' and 'Personal data.' Data subject refers to the living individual to whom the personal data relates to. Data controller refers to the person/persons who are responsible for determining the purpose for which the data is to be used or processed. Data Processor refers to the collection and manipulation of all the items present in the data in order to provide meaningful information. At this juncture, it has to be clearly understood that there is a difference between 'Personal data' and 'Sensitive Personal data.' Sensitive Personal data refers to the information (pertaining to individuals) regarding their physical or mental health, political opinions, religious beliefs and radical & ethnic origin of the data subject.

The Freedom of Information Act (FOIA) was adopted in 2000 enjoining the formation of an information commission. The first schedule of the DPA states that the personal data (of the individuals) shall be processed fairly and lawfully. It also states that personal data can be processed only when certain conditions are fulfilled. Firstly, there must be certain legitimate grounds for collecting personal information of the individuals. Secondly,

[84] Data Protection Directive, Art. 8 (2) and GDPR Article 9.
[85] Pursuant to the EU Data Protection Directive 95/46/EC.

individuals/organisations (collecting personal data) should be transparent regarding the usage of the personal data. Thirdly, the personal data should be handled in a manner which the individuals (from whom personal data is collected) would reasonably expect. Lastly, the organisations/individuals responsible for processing the personal data should not indulge in any act which would lead to the unlawful use of the data. The DPA describes itself as being an Act that makes *'new provision for the regulation of the processing of the information relating to individuals'.* This statement is worth thinking about, for it has massive ramifications. The DPA forms part of a comprehensive and harmonized European legal framework for the regulation of the processing of personal data. This framework is a consequence of work done by the Council of Europe and the EC. But, still it is a surprise that DPA hasn't tried to define the meaning of the word 'privacy.'[86] Further, the DPA does not regulate the processing of information relating to unidentified or unidentifiable living individuals, or the processing of information relating to the deceased or the processing of information relating to companies, non-incorporated organizations (such as clubs and societies), public authorities, charities or similar bodies.[87] The data protection principles set out for processing of personal information required that the processing is fair and lawful, that the data are collected and used only for specific and lawful purposes, that the data are adequate and relevant for the purpose for which they are collected, that accuracy of the data is maintained, that they are not retained unless necessary, that they are kept secure and not transferred to third countries.

The DPA aims at regularising the processing of information pertaining to individuals (including obtaining or disclosure of the information pertaining to those individuals). But, it does not put a bar on the disclosure of personal data. Thus, personal data can be disclosed if it is consistent with the purpose for which it is obtained. This means that the person to whom the

[86] Stewart Room, *Data protection and compliance in context*, BCS, The Chartered Institute for IT; 1 edition (November 27, 2006), p.3.
[87] Stewart Room, *Data protection and compliance in context*, BCS, The Chartered Institute for IT; 1 edition (November 27, 2006), p.1.

information is disclosed intends to use the information in the same manner as it was intended at the time of collection.

CONCLUSION

There is a need to abolish the practice of biometrics information and to adopt other methods of collecting general information. In the absence of stringent laws for data protection, personal information of individuals should not be taken by the government. The author is more concerned for the security of the personal data which, in the absence of data protection laws, is at stake. A citizen under this right has the right to protect and safeguard the liberty of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. Privacy is a very wide concept. It includes the private space (such as the home), private items (such as letters and photographs), private relationships (such as sexual relationship) and private information (such as information about people). The government is slowly but surely evolving into electronic governance models. The key challenge in balancing of competitive rights is evolving a test that would determine the balance that would secure the ends of justice and public interest at large. The author opines that even in the case of privacy, *the proportionality test* would succeed in giving the best results especially in cases concerning freedom of expression. The doctrine of proportionality is an accepted principle in Indian law. The genesis of the doctrine is in administrative law. The test involves the weighing of the countervailing consideration involved in a particular case. Further, the court ought to come to the conclusion that the infringement is justified. The Supreme Court speaking through a five-judge bench in the *Sahara case*[88] accepted the doctrine of proportionality and applied it to balance the right to fair trial and the freedom of expression. The right to respect for personal privacy is a recognized human right. Though right to privacy has been recognized by many judgements to be implicit under Part III of the constitution, there is a need to explicitly adopt

[88] (2012) 10 SCC 603: (2013) 1 SCC (L&S) 76: (2013) 1 SCC (Civ) 173.

right to privacy as a fundamental right by the parliament. Despite the right to privacy being accorded judicial recognition time and again, there still does not exist a cogent legal framework for privacy laws in India. Not only the Judiciary, but also the legislature at certain instances has recognized the essential right to privacy and the need to make it a statutory right. However, for it to become a fundamental right, the Parliament needs to make a constitutional amendment to that effect and finally give the citizens of India the unequivocal and paramount right to protect their privacy from any external interference.