LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +918255090897 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

PUNISHMENT AADHAAR AND THE GARROTTING OF INDIVIDUAL PRIVACY*

The Government's new mass surveillance systems Aadhaar present new threats to the right to privacy. Mass interception of communication, keyword searches and easy access to particular users data suggest that state is moving towards unfettered large-scale monitoring of communication. The paper aims to achieve a comprehensive, doctrinal understanding of the constitutional right to privacy, as developed, understood and implemented by the judiciary, which is an essential prerequisite to embarking upon a legality and constitutionality of Aadhaar. Part II of this paper covers discussions of privacy in the context of our fundamental rights by the draftspersons of our constitution, and then moves on to the ways in which the Supreme Court of India has been reading the right to privacy into the constitution. Part III discusses how Aadhaar in present form would encroach upon Individual privacy. Whether inevitable privacy concerns arising out of such a data collection exercise have been dealt with in a meaningful and comprehensive manner? Part IV throws light on claim, can Fundamental Rights be waived by the people for the sake of accessing welfare benefits? The part V while concluding makes a case for expanding our existing privacy safeguards to protect the right to privacy in a meaningful manner in face of state surveillance.

I. INTRODUCTION

We are in an age where we live in what the legal theorist, Bernard Harcourt, has in his book[1], called the 'expository society'. We hunger for exposure as well as the better fulfilment of our cravings obliges us to surrender privacy. But even the craving for the satisfaction of our desires should not make us immune from worrying about how power is exercised over us. In its crude instrumentalism about constitutional propriety and privacy, the Aadhaar bill is a demonstration of just how easily state power can become arbitrary. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 though intends to provide for targeted delivery of subsidies and services to individuals residing in India[2] leaves many thing unsaid as it was a sold to the public based on the claim that enrolment was 'voluntary'. This basically meant that there was no legal compulsion to enrol. But Aadhaar was made mandatory for an ever-widening range of facilities and services[3]. However, in March 2014, the court ruled

* **Mr. Shubham Chaudhary, 4th Year, B.A LL.B (Hons.), Dr. RML National Law University, Lucknow**

[1] Bernard Harcourt, Exposed, Desire and Disobedience in the Digital Age (2015).

[2] PrsIndia, *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016*, available at http://www.prsindia.org/billtrack/the-aadhaar-targeted-delivery-of-financial-and-other-subsidies-benefits-and-services-bill-2016-4202/ (Last visited on January 25, 2017).

[3] Aadhaar Bill § 7 (2016).

that 'no person shall be deprived of any service for want of Aadhaar number in case she is otherwise eligible'[4].

Whilst there are a number of controversies relating to the Aadhaar Bill, including the fact that it was introduced as money bill so as to circumvent the majority of the opposition in the upper house of the Parliament and was rushed through the Lok Sabha in a mere eight days[5]. but most disturbing tend to be remark made by the Attorney general while defending it in Supreme Court that we have no Right to privacy and privacy has been a 'vague' concept all these years. The court didn't answer this questions involved in the matter at hand, and it referred to a larger bench of at least 5 judges to decide. It is truly unfortunate that the privacy debate in India is circling back to its initial stages in 1948-49.

II. RIGHT TO PRIVACY IN INDIA

The term 'Privacy' has been described as the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others.[6] The concept is used to describe not only rights purely in the private domain between individuals but also constitutional rights against the State.[7] The need for privacy and its recognition as a right is a modern phenomenon. It is the product of an increasingly individualistic society in which the focus has shifted from society to the individual. In early times, the law afforded protection only against physical interference with a person or his property. As civilisation progressed, the personal, intellectual and spiritual facets of the human personality gained recognition and the scope of the law expanded to give protection to these needs.

A. THE CONSTITUENT ASSEMBLY AND THE RIGHT TO PRIVACY

The Constituent Assembly did not take the right to privacy as seriously as it should have whilst crafting the Fundamental Rights. This may have been a direct result of the relative scarcity of material on the right to privacy at the time. An amendment to insert the right against unreasonable searches was very nearly passed by the house, but ended up being dropped. Two different forms of privacy were proposed as insertions to the Fundamental Rights Chapter of the Constitution and both were rejected with very little debate. One of these was to do with safeguards against unreasonable search and the other protected the privacy of correspondence. The amendment to embed safeguards against arbitrary search and seizure in the Indian Constitution was moved by Kazi Syed Karimuddin[8]. Dr. Ambedkar was willing to accept Karimuddin's proposal. He pointed out that this clause was already in the Criminal Procedure Code, and was therefore a part of Indian law, but also acknowledged that it may be desirable in the interests of personal liberty to 'place these provisions beyond the reach of the legislature[9]. The chaos during voting over the proposal suggests that it was contentious. The Vice-President attempted twice to put the Karimuddin text to vote[10]. Although he declared the amendment as

[4] Jean Dreze, *the Aadhaar coup,* March 15, 2016, available at http://www.thehindu.com/opinion/lead/jean-dreze-on-aadhaar-mass-surveillance-data-collection/article8352912.ece (Last visited on January 24, 2017).
[5] M.R. Madhvan, *The power to certify*, available at http://www.thehindu.com/todays-paper/tp-opinion/the-power-to-certify/article8604916.ec, (Last visited on January 25, 2017).
[6] Adam Carlyle Breckenridge, the Right to Privacy, (1971).
[7] Edward Shils, Privacy: Its Constitution and Vicissitudes, (1966), Law and Contemporary Problems 31, No.2
[8] Amendment 512 moved by Kazi Syed Karimuddin, Constituent Assembly Debates, Volume VII, Constituent Assembly Of India (3-12-1948).
[9] Id.
[10] Id.

having been accepted both times, Mr. T.T Krishnamachari objected, saying both times that the majority vote was of those who were not in favour of the amendment[11]. The records of the day's debates suggest that there was unrest in the house at the time. Jawaharlal Nehru supported a proposal to postpone the vote, and the vote was postponed accordingly[12].This incident proved controversial later on, and objections were raised over the manner in which the vote was shelved. Eventually Karimuddin's amendment was put to vote on a different day with no debate, and was defeated.[13] The consequence was that the privacy principles safeguarding citizens from intrusive search and seizure were never inserted in the Constitution. The records of the Constituent Assembly debates are therefore disappointing if one is seeking powerful reasoning to explain the omission of the right to privacy.

B. THE RIGHT TO PRIVACY: DEVELOPMENT THROUGH CASE LAW

While the constitution Assembly Debate and the choices made about the Fundamental Rights were still fresh in public memory in 1954, the apex court refused to read the right to privacy in *M.P Sharma v. Satish Chandra*[14]. It is one of the two cases cited by Attorney General claiming that there was no Fundamental right to privacy under the Indian constitution[15]. In my opinion, this case from 1954 had nothing to with the determination of the issue, i.e., whether or not the Constitution recognised privacy as a fundamental right. Instead, it was a challenge to the search warrant issued by the District Magistrate in Delhi to the Delhi Special Police Establishment to investigate a case relating to embezzlement of funds by a private company and its associated companies. Nine Judge Constitutional Bench, headed by the then Chief Justice M C Mahajan held that the search warrants were legal and necessary. They also held that such lawfully issued search warrants did not violate any fundamental right guaranteed by the Constitution. While saying so, they put in just one line about privacy: "*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*."

To hold that this amounts to an authoritative denial that there is a fundamental right to privacy guaranteed by the Constitution would be stretching the Court's words beyond what they intended to imply. The Court was only stating a factual point that right to privacy is not listed in the fundamental rights chapter and they do not propose to import it into another extant fundamental right. In my opinion it would be not only crafty but also dangerous to interpret this one-liner to mean that a precedent had been set by the Court on this issue saying that the Court had rejected the idea of the fundamental right to privacy. They simply did not want to interpret the existing fundamental rights to discover the right to privacy.

The next case reportedly cited by the AGI is the Court's view in *Kharak Singh vs State of U.P. and Ors.*[16] In this case the Petitioner, challenged the Uttar Pradesh Police Regulations under which the Police frequently visited his house at unearthly hours and compelled him to go to the police station. Writing the majority opinion for the Constitution Bench headed by the then Chief Justice B P Sinha held that there was no violation of the Petitioner's right under Article

[11] Constituent Assembly Debates, Volume VII, Constituent Assembly of India (3-12-1948).
[12] Id.
[13] Constituent Assembly Debates, Volume VII, Part II Constituent Assembly of India (6-12-1948).
[14] M.P Sharma v. Satish Chandra, AIR 1954 SC300.
[15] Krishnadas Rajgopal, Privacy not a right, Aadhaar legit, July 23, 2015, available at http://www.thehindu.com/news/national/privacy-not-a-right-aadhaar-legit-centre/article7452839.ece (Last visited on January 25, 2017).
[16] Kharak Singh vs State of U.P. and Ors, AIR 1963 SC 1295.

19(1) (d) because that article refers to "*something tangible and physical rather and not to the imponderable effect on the mind of a person which might guide his action in the matter of his movement.*" However the majority held that the impugned Regulation violated the right to liberty guaranteed under Article 21 as it was not based on any law. In support of this finding the Court opined "*We have already extracted a passage from the judgment of Field, J. in Munn v. Illinois, where the learned judge pointed out that 'life' in the 5th and 14th Amendments of the U. S. Constitution corresponding to Art. 21, means not merely the right to the continuance of a person's animal existence, but a right to the possession of each of his organs-his arms and legs etc."* The finding required the Court to interpret the meaning of the term 'personal liberty' in Article 21. By contrasting the very specific rights listed in Article 21, the Court held that*: "Is then the word 'personal liberty' to be construed as excluding from its purview an invasion on the part of the police of the sanctity of a man's home and an intrusion into his personal security and his right to sleep which is the normal comfort and a dire necessity for human existence even as an animal? It might not be inappropriate to refer here to the words of the preamble to the Constitution that it is designed to 'assure the dignity of the individual' and therefore of those cherished human value as the means of ensuring his full development and evolution. We are referring to these objectives of the framers merely to draw attention to the concepts underlying the constitution which would point to such vital words as 'personal liberty' having to be construed in a reasonable manner and to be attributed that these which would promote and achieve those objectives and by no means to stretch the meaning of the phrase to square with any preconceived notions or doctrinaire constitutional theories"*

To hold that in this case the Apex Court had ruled against the fundamental right to privacy may amount to a complete misunderstanding of the thinking of the Court as well as attributing to it an opinion that it never expressed in the first place. The deep concern over the need for protection of an individual's freedoms against the unbridled exercise of State power by its agents and the relief provided by striking down the offending regulation as ultra vires of the Constitution clarifies the Court's views on the issue of an individual's privacy which are understood as personal liberties within the meaning of Article 21 of the Constitution. They only stopped short of declaring it as an implied fundamental right. In his partly concurring and partly dissenting opinion, Subba Rao, J. went one further, by holding that the idea of privacy was, in fact, contained within the meaning of Article 21, "*It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty."*

Watershed moment for Indian privacy law came with *Gobind v. State of M.P*[17], decided in 1975, Like *Kharak Singh, Gobind* also involved domiciliary visits to the house of a history-sheeter. The surveillance provisions in the impugned regulations, according to the Court, were indeed for the purpose of preventing offences, since they were specifically aimed at repeat offenders. The Court held *"the right to privacy must encompass and protect the personal intimacies of the home, the family marriage, motherhood, procreation and child rearing. This catalogue approach to the question is obviously not as instructive as it does not give analytical picture of that distinctive characteristics of the right of privacy. Perhaps, the only suggestion that can be offered as unifying principle underlying the concept has been the assertion that a claimed right must be a fundamental right implicit in the concept of ordered liberty· The right to privacy in any event will necessarily have to go through a process of case-by-case development".* However, the Court examined the grounds for limiting the right to privacy. It held*: "Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right, that fundamental right must be subject to restriction on the basis of compelling public interest."*

[17] Gobind v. State of M.P (1975) 2 SCC 148.

Thus, *Gobind* essentially crystallized a constitutional right to privacy as an aspect of personal liberty, to be infringed only by a narrowly-tailored law that served a compelling state interest. Soon afterwards, *R. Rajagopal v. State of T.N*[18] involved the question of the publication of a convicted criminal's autobiography by a publishing house. Technically, this wasn't an Article 21 case. The Court itself made things clear when it held that the right of privacy has two aspects: the tortious aspect, which provides damages for a breach of individual privacy; and the constitutional aspect, which protects privacy against unlawful governmental intrusion. Having made this distinction, the Court went on to cite a number of American cases that were precisely about the right to privacy against governmental intrusion, and therefore & ideally & irrelevant to the present case and then, without quite explaining how it was using these cases & or whether they were relevant at all, it switched to examining the law of defamation. It would be safe to conclude, therefore, in light of the clear distinctions that it made, the Court was concerned in *Rajagopal* about an action between private parties, and therefore, privacy in the context of tort law. In 1997, the Supreme Court decided *PUCL v. Union of India*.[19] This case is the most important privacy case after *Gobind*. In *PUCL*, the constitutionality of Section 5(2) of the Telegraph Act was at issue which authorise intercepting and phone tapping. The Court held unambiguously that individuals had a privacy interest in the content of their telephone communications. It cited Kharak Singh, Gobind and Rajagopal for the proposition that privacy was a protected right under Article 21. Privacy restrictions must be narrowly tailored, if they are to be constitutional. Therefore, the Court continues with the strong privacy-protection standards developed in *Gobind* and afterwards. Cases after *PUCL* are a mixed bag. *Collector v. Canara Bank*[20], decided in 2005. In that case, Court made an obiter observation "*the right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in Bank, must continue to remain confidential vis-à-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank ".* One things stand out, an affirmation that the right is one that vests in persons and the Court requires reasonable suspicion before the surveillance in question is undertaken. Following on from *Canara Bank,* in *P.R Metrani v. CIT*[21], a search and seizure provision in the Income Tax Act (Section 132(5)) was construed strictly as it constituted a "serious invasion into the privacy of a citizen. *Selvi v. State of Karnataka*[22], decided in 2010, involved the constitutionality of Narco-analysis and polygraph tests during police investigations, and the testimonial statements obtained therefrom. The Court had no trouble in finding that, insofar as these techniques interfered with a person's mental processes in order to elicit information from him, they infringed his right to privacy. Recently, in *Ramlila Maidan Incident, In re*[23], the Apex Court cited its previous decisions (including PUCL) to hold that the right to privacy has been held to be a fundamental right of the citizen and a part of life under Article 21.

Despite the diversity of cases and the differing reasoning employed by judges to reach differing results over time, we have seen that a careful analysis reveals certain unifying strands of logic and argument that can provide a coherent philosophical and constitutional grounding to the right to privacy in Indian law.

III. PRIVACY CONCERNS IN AADHAAR

[18] R. Rajagopal v. State of T.N (1994) 6 SCC 632.
[19] People's Union for Civil Liberties v. Union of India, 1 SCC 301.
[20] Collector v. Canara Bank (2005) 1 SCC 496.
[21] P.R Metrani v. CIT (2007) 1 SCC 789.
[22] Selvi v. State of Karnataka, (2010) 7 SCC 263.
[23] Ramlila Maidan Incident, In re (2012) 5 SCC 1.

Initially, Privacy concerns were raised by the Parliamentary Standing Committee on Finance which in 2011 rejected the National Identification Authority of India (NIAI) Bill 2010 on the basis of privacy, feasibility, uncertainty[24]. Yet, the government did not attempt to modify the Bill and bring it back for parliamentary approval. This part discuss the substantial aspects of the Bill in relation to privacy concerns which have been raised by a number of experts.

A. MASS SURVEILLANCE AND TRACKING OF INDIVIDUALS

This Aadhaar number is unique in that it corresponds to biometrics which may be used by an individual throughout his/her life for all major transactions. This in itself has led to concerns of it enabling tracking of individuals by the Government. The Indian Bill makes no such explicit reference, however, the fact that such a record will be maintained may be inferred from Section 33, which states that the Authority may be required to share 'identity information' along with 'details of authentication' the latter referring to all requests for authentication of identity which have been received by the UIDAI. This record may be compared to that of an 'trail', as such records will reveal much about the 'Aadhaar' number holder's daily activities from accessing the PDS, to bank records, travel records, and even education records as per the most recent MoU signed with the HRD Ministry.[25] It will be child's play for intelligence agencies to track anyone and everyone where we live, when we move, which events we attend, whom we marry or meet or talk to on the phone.. No other country, and certainly no democratic country, has ever held its own citizens hostage to such a powerful infrastructure of surveillance and infringes privacy of its citizen at such a level.

B. CONVERGENCE AND PROFILING OF INDIVIDUALS

Information about individuals that are given to companies, banks, governmental agencies and departments are held in 'silos', discrete towers which hold specific information provided for a specific purpose/service (Driving License, Voter ID Card, Ration Card). Experts opine that the UID will serve to link all the discrete silos, a process known as 'convergence', and therefore unleash the capability to profile an individual on the basis of personal data.[26] Convergence of information allows third parties, including private companies to utilize such information to harass a person. A common example is the way private companies obtain access of personal details of individuals and pursue aggressive marketing strategies through phone and email in ways that intrude upon their privacy. In fact, one of the selling points of the project has been that the Aadhaar numbers will enable de-duplication of other databases as well such as the National Population Register for example. This necessarily involves convergence with duplicate-infested erroneous data.[27] It is clear that convergence of data is an integral part of the UID project, which many see as a tool which may be put to intrusive purposes.

C. NATIONAL SECURITY RATIONALE OF THE UID

National security finds no mention in the Statement of Objects of the Bill. However, the Statement of Objects and Reasons remain an external aid to interpretation of a Statute[28] and Section 33(b) of the Bill widens the objectives that the Act seeks to achieve. It allows for disclosure of information possessed in the CIDR if it is made 'in the interests of national security' pursuance of a direction to that effect issued by an officer not below the rank of Joint

[24] The Hindu, *Blow to Aadhaar project as Bill is rejected*, available at http://www.thehindu.com/news/national/blow-to-aadhaar-project-as-bill-is-rejected/article2698907.ece, December 8, 2011, (Last visited on January 21, 2017).
[25] *HRD Ministry signs MOU with UIDAI*, The Economic Times (Delhi), October 27, 2010.
[26] Usha Ramanathan, A Unique Identity Bill, Economic and Political Weekly (Mumbai), July 24, 2010, 10-14.
[27] Ruchi Gupta, Justifying the UIDAI: A Case of PR over Substance? Economic and Political Weekly (Mumbai), October 2, 2010, 136.
[28] GP Singh, Principles of Statutory Interpretation, 238.

Secretary or equivalent in the Central Government after obtaining approval of the Minister in charge. Before any such direction can take effect, it will be reviewed by an oversight committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology. The National security exceptions in the bill are too broad. In 1996, the Supreme Court interpreted provisions under the Indian Telegraph Act, 1885 with regard to the state being allowed to tap telephones. The Court held that the state may tap telephones only at the occurrence of any public emergency or in the interest of public safety if: (i) it is authorised by the Home Secretary of the central or state government; and (ii) it is for a maximum period of six months. The Bill differs from the guidelines for phone tapping in the following two ways. First, the Bill permits sharing in the interest of 'national security' rather than for public emergency or public safety. Second, the order can be issued by an officer of the rank of Joint Secretary, instead of a Home Secretary. Under the Indian Telegraph Act, 1885 it is only in 'urgent situations' that directions for phone tapping may be given by a Joint Secretary.[29]

But, more importantly, let us say you do want a national security exception. Should the determination of this be left entirely to the bureaucracy and executive when they themselves will not be under any system of accountability? There is no effective independent, credible mechanism for holding accountable those who will be making determinations on this exception. So essentially, a small group of bureaucrats can render your privacy irrelevant. The Supreme Court was right in *PUCL*[30] that each order of telephone tapping must also be investigated by a separate Review Committee within a period of two months from the date of issuance. The UN High Commissioner for Human Rights Navi Pillay published detailed report on 'The Right to Privacy in the Digital Age' in July 2014. The report stated clearly that internal procedural safeguards without independent external monitoring are inadequate for the protection of rights.[31] But the said effective independent & separate review committee was lacking in the Bill, unlike United States' Foreign Intelligence Surveillance Court (1978) and United Kingdom's Investigatory Powers Tribunal (2008) Agencies to oversee and examine unlawful surveillance in respective countries.[32] Making situation worse is Section 47(1) of the Bill which excludes courts from taking cognisance of offences under the legislation, requiring that the authority that runs Aadhaar consent to prosecution for any action to be taken under the legislation[33]. This part of the Bill completely undermines all the safeguards that do exist within it, since citizens cannot access these safeguards without co-operation from the authority which is arguably in a position of conflict of interest.[34] There may be situations in which members or employees of the UID authority are responsible for a security breach.

D. BIOMETRIC INFORMATION IN THE HANDS OF PRIVATE PLAYERS

The procedure adopted by UIDAI is so casual that it borders on irresponsibility. Briefly, the entire process at the field level is in the hands of private enterprises known as enrollers who operate freely without any government supervision. The biometrics are initially stored and

[29] People's Union for Civil Liberties (PUCL) v. Union of India. (1997) 1 SCC 301 (India).
[30] Id.
[31] Navi Pillay, *Press Conference on the right to privacy in the digital age UN High Commissioner for Human Rights*, available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14874, (Last visited on January 14, 2017).
[32] P Arun, *Can the Aadhaar Bill Be Used By the Govt. As An Excuse to Violate Our Right to Privacy*, March 11, 2016 available at http://www.youthkiawaaz.com/2016/03/aadhaar-data-surveillance-privacy-national-security/ (Last visited on January 14, 2017).
[33] Aadhaar Bill § 47 (2016).
[34] Chinmayu Arun, *Privacy is a fundamental right*, March 18, 2016, available at http://www.thehindu.com/opinion/lead/lead-article-on-aadhaar-bill-by-chinmayi-arun-privacy-is-a-fundamental-right/article8366413.ece (Last visited on January 16, 2017).

collected in private hands before it is transmitted to the UIDAI Central ID Repository (CIDR). The UIDAI has no privity with the enrolling agencies. The loose framework of relationships linking UIDAI to the collection of biometric data is through MOUs with state governments or departments known as registrars. It is these registrars who engage private sector enrolment agencies. Our biometrics are handled by entities of alien origin with no particular affection for Indian Constitutional values. If a private entity is involved in the maintenance and establishment of the CIDR it can be presumed that there is the possibility that they would, to some degree, have access to the information stored in the CIDR, yet there are no clear standards in the Act regarding this potential access. The fact that the UIDAI has been given the freedom to appoint an outside entity to maintain a sensitive asset such as the CIDR raises security concerns.

E. VIOLATING PRIVACY PRINCIPLES ENUMERATED BY JUSTICE AP SHAH COMMISSION

In 2011, the erstwhile Planning Commission constituted a group of experts to suggest the contours of future Indian privacy law. Chaired by Justice AP Shah, the group considered the implications of the Aadhaar project and proposed nine principles to inform privacy law, thereby serving as an excellent frame of reference for any legislation such as the Aadhaar Bill 2016 that raise substantive privacy concern[35]. Such National privacy Principles are the extension and improvisation of the similar principles laid down by the Draft Bill 2011[36]. One of the principle provides individuals should have access to personal information about them held by an entity governed by the Act and the ability to seek correction, amendments, or deletion of such information where it is inaccurate. The Aadhaar Act provides that Aadhaar number holders may request the UIDAI to provide access to their identity information expect their core biometric information[37]. It is not clear why access to the core biometric information[38] is not provided to an individual. It may also be noted that the Aadhaar Act provides only for a request to the UIDAI for access to the information and does not make access to the information a right of the individual, this would mean that it would be entirely upon the discretion of the UIDAI to refuse to grant access to the information once a request has been made. Another Privacy principle infringes by Aadhaar Bill involves Consent principle it says Information must only be disclosed to third parties after notice and informed consent is obtained. Though Aadhaar Bill creates a blanket prohibition on the usage of core biometric information for any purpose other than generation of Aadhaar numbers and also prohibits its sharing for any reason whatsoever[39]. The prohibition on disclosure of information (except for core biometric information) does not apply in case of any disclosure made pursuant to an order of a court not below that of a District Judge[40]. There is another exception to the prohibition on disclosure of information in the interest of national security if so directed by an officer not below the rank of a Joint Secretary to the Government of India[41]. It does not involve the consent of the individual; however, given the capability of misuse of this provision it has been urged that the

[35] Justice AP Shah, *Group of expert on privacy*, available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf , October 16, 2012 (Last visited on January 23, 2017).

[36] Centre for Internet and Society, *An Analysis of the New Draft Privacy Bill*, available at http://www.medianama.com/2014/03/223-an-analysis-of-the-new-draft-privacy-bill-cis-india/, March 28, 2014, (Last visited on January 22, 2017).

[37] Aadhaar Bill § 28 (2016).

[38] Core biometric information is defined as fingerprints, iris scan or other biological attributes which may be specified by regulations.

[39] Aadhaar Bill § 29(1) (2016).

[40] Aadhaar Bill § 33(1) (2016).

[41] Aadhaar Bill § 33(20 (2016).

concerned person should at least be given the right to be notified of such disclosure in advance, or generally be given an opportunity to resist the same.

The champions of the Aadhaar Bill downplay these concerns for the sake of enabling the government to save some money. Wild claims are being made about Aadhaar power to plug leakages. In reality, Aadhaar can only help to plug specific types of leakages. It is true that developmental schemes such as the NREGA, and PDS faced hindrances due to identification of beneficiaries, it was not the existence of 'identification proof that posed a problem, as much as fraud, collusion between middlemen and labourers etc. that did.[42]

IV. BETWEEN ROCK AND WHIRLPOOL

K.K. Venugopal, appearing with Attorney general even argue that even if privacy was a fundamental right, the Aadhaar beneficiaries would not mind waiving it for the sake of accessing welfare benefits. He also submitted that the court could not insist that the beneficiary retain the right to privacy if he wanted to waive it. Can an individual voluntarily waive his right to privacy by enrolling for Aadhaar? The Supreme Court in *Behram v State of Maharashtra*[43] examined this question and stated that fundamental rights were not kept in the Constitution merely for individual benefits. Fundamental rights were a matter of public policy and thus, the doctrine of waiver does not apply in case of fundamental rights. In other words, a citizen cannot 'give up' his fundamental rights. Later, in the *Basheshar Nath* case[44], court, limiting their decision to Article 14, held that the right conferred by the article, could not be waived. Justice Bhagwati went a step further and stated that the Constitution was 'sacrosanct', that it would be a 'sacrilege' to whittle down fundamental rights and that it was the 'sacred' duty of the Supreme Court to safeguard fundamental rights. The court held that the Constitution makes no distinction between the fundamental rights enacted for the benefit of an individual and fundamental rights enacted for the benefit of the public. This position has been subsequently reiterated in *Olga Tellis*[45]. Is it morally right for a government to insist on the waiver of fundamental rights for accessing benefits? The Supreme Court in 1974 elaborated the doctrine of unconstitutional conditions in Ahmedabad St Xavier's College v State of Gujarat as "any stipulation imposed upon the grant of a governmental privilege which in effect requires the recipient of the privilege to relinquish some constitutional right.[46]

V. CONCLUSION: NO EXCUSE FOR INEFFECTIVE SAFEGUARDS

The Aadhaar project in my perception, annihilate the social contract that underlies the Indian Constitution. If there is a moral theory on which our Constitution rests, it is the theory that there are limits to State power and there are certain boundaries that the State cannot transgress, no matter how great the perceived benefit be. Indian citizens have rights against the State and against each other. The right to be left alone, the right to be silent, the right to be anonymous are aspects of individual liberty that are slip siding away due to technologies that most of us

[42] Reetika Khera, *Not all that unique*, August 30, 2010, available at http://www.hindustantimes.com/Not-all-that-unique/Article1-593541.aspx (Last visited on January 09, 2017).
[43] Behram v State of Maharashtra, AIR 1955 SC 123.
[44] Basheshar Nath v. Commissioner of Income Tax, AIR 1959 SC 149.
[45] Olga Tellis v. Bombay Municipal Corporation, AIR 1986 SC 180.
[46] Juma sen, *Why Aadhar's Backers are Wrong to Say Privacy Rights Can be Voluntarily Waived, October 10, 2015, available at* http://thewire.in/2015/10/09/why-aadhars-backers-are-wrong-to-say-privacy-rights-can-be-voluntarily-waived-12769/ (Last visited on January 14, 2017).

can barely comprehend. Aadhaar isn't right since it bargains the real uprightness of each of us by grabbing endlessly a personal part of our physical character. It is wrong because it is no part of the business of the Government of India to create a vast data bank of biometrics that can be used and abused against Indians. The Aadhaar project with its colossal capability of reconnaissance adjusts the relationship amongst subject and state. It tilts the balance so steeply in favour of government that a citizen whose biometrics are controlled by the State is permanently condemned to submission. A central bank of biometric data robs individuals of dignity assured by the Preamble to the Constitution.

Despite the fact that the bill has been passed in Parliament, it is imperative to keep up the weight so that we can frame better regulations and seek judicial protection. The proposed bill raises several questions, which need to be analysed profoundly. Instead of disruptive discussions, this bill should have be dealt with critical discussion in the Parliament before its passage On the off chance that this bill get through Supreme Court scrutiny with the same provisions, it would have a drastic impact on security and privacy. It is to be hoped that the Supreme Court perceives the damage that unrestrained mass surveillance will wreak on our democracy, and that it takes its jurisprudence forward by several steps unimpeded by its own initial reluctance to create powerful safeguards in PUCL telephone tapping case. If so then, in my opinion the issue whether Aadhaar card intrudes an individual's privacy should be tested under the triple test stated in Maneka Gandhi's case[47]. These are first, it must prescribe a procedure; second, the procedure must withstand the test of one or more of the fundamental rights conferred under Article 19 which may be applicable in a given situation; and third, it must withstand the equality test of Article 14. This is very much the reading for the law and procedure authorising interference with personal liberty and right of privacy – that it should be right, just and fair and not arbitrary, fanciful or oppressive.

Therefore, only comprehensive renovation of the Aadhaar Bill to build within it the principles of justice, fairness, and reasonableness will able to suffice the inner conscience. Notwithstanding, genuine national interest may dictate that laws on data/digital privacy protection and cyber security be urgently enacted and linked with the Aadhaar Bill, before it becomes operational in the public sphere.

[47] [AIR 1978 SC 597]