

## RIGHT TO PRIVACY: REDEFINING SOCIAL SECURITY IN INDIA

Satya Vrat Yadav and Vasundhara Anil Kaul<sup>1</sup>

### **Abstract**

*Privacy has been defined in several ways over last hundreds of years. Judge Thomas Cooley called it as a right to be let alone. Time and again philosophers, scholars and Jurists tried to lament the difficulty to satisfy the concept of privacy. Aurther Miller in his work has declared privacy as difficult to define as its nature is exasperatingly vague and evanescent. Privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.*

*Indian polity has been continuously debating on merits and demerits of clouding data of one and all citizens of the country through UID system ever since the concept of ADHAAR has been introduced. This UID system carry necessary biometric data, which if falls in the wrong hands can be very dangerous to the society. It's one of the few possible consequences may be identity theft.*

### **Introduction**

---

<sup>1</sup> College of Legal Studies, University of Petroleum and Energy Studies, Kandoli, Via Prem Nagar, Dehradun, Uttarakhand - 248007

Privacy has been defined in several ways over hundreds of years. Judge Thomas Cooley<sup>2</sup> called it as a right to be let alone<sup>3</sup>. Time and again philosophers, scholars and Jurists tried to lament the difficulty to satisfy the concept of privacy. Further Miller in his work "*the assault to Privacy*" has declared privacy as difficult to define as its nature is exasperatingly vague and evanescent<sup>4</sup>. Privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.

Indian polity has been continuously debating on merits and demerits of clouding data of one and all citizens of the country through UID system ever since the concept of ADHAAR has been introduced. This UID system carry necessary biometric data, which if falls in the wrong hands can be very dangerous to the society. It's one of the few possible consequences may be identity theft.

There are three main issues which have been haunting the issue of privacy all the time after introduction of UIDAI:

First, Centre has been collecting all personal biometric data without any legal authority or in other words without any statute backing it. Even now there is no legislation enforced; however Aadhaar bill 2016 has been tabled enacted but a lot of process needs to be followed to make this half cooked idea ready for being severed.

Second, UIDAI used many private parties to enroll and collect biometrics from people. There can be no guarantee that the some of the collected biometric data will not remain in private hands, leading to the possibility of misuse.

The main and foremost issue that stands here is as to whether Right to privacy is vested in the citizens or not well, this issue of right to privacy is in the court and has to be decided by the Supreme appellate authority of the country. In past there have been a number of judgments by honorable Supreme Court which read right to privacy as part of right to life<sup>5</sup>, contradicting the eight Judges bench of honorable Apex Court which first ruled for absence of any such right<sup>6</sup>.

On introduction of UID, it was stipulated by the scholars and eminent legal personalities, that this accumulation of data may be a threat to individual protection. Scholars drew a prime link of association between UID and national security. Government has been calming time and time again of this data collection and Aadhaar scheme being voluntary but the way, they are

---

<sup>2</sup>Thomas Cooley, United state Jurist, <http://www.britannica.com/biography/Thomas-Cooley> (Last visited May 5, 2016)

<sup>3</sup> United Kingdom Privacy Laws, <http://www.leeds.ac.uk/law/hamlyn/princess.htm>, (Last Visited May 5, 2016)

<sup>4</sup>Charles R. Ashman, *The Assault on Privacy* by Arthur R. Miller, vol. 20, DePaul Law Review, 1971, <http://via.library.depaul.edu/cgi/viewcontent.cgi?article=2982&context=law-review> (Last seen May 5, 2016)

<sup>5</sup>Govind v. State of Madhya Pradesh, AIR 1975 SC 1378; R. Rajagopal v. State of Tamil Nadu, 1994 SCC (6) 632

<sup>6</sup>Kharak Singh v. State of Uttar Pradesh, (1964) SCR (1) 332

mandating this biometric lashed UID to avail any social welfare service run by government, their stand is quite clear that in near future Aadhaar is going to be a most important document to survive in the country.

It can be clearly fragmented from the scenario that there may be two particular infringement of security inalienable in the UID framework: union of data and assent. The UID database makes it feasible for the connecting or joining of data crosswise over storehouses. What's more, assent is unaccounted for in the UID framework. "Aadhaar is a huge database of biometric and different points of interest of a great many individuals; the issue that needs consideration is, since holders of information should be legitimately in charge of the information that they gather and hang for the information suppliers. The absence of authoritative investigation and in this manner administrative authorization for this anticipates is alarming. Even after the enactment of the legislation, there are no legitimate commitments on the Unique Identification Authority of India on the utilization of this information, either as far as its trustworthiness or for ensuring the national separating with touchy information."

### **The right to privacy**

The absence of an enactment ensuring the privilege to protection in India likewise turns into a variable to consider. Keeping up biometric information of more than 100 crores Indians with no legitimate commitment to keep up protection is by a wide margin the most convincing contention against Aadhaar. In a post-Snowden world, in what capacity can something as argumentative as Aadhaar, be permitted to take roots without even as much as a parliamentary dialog?

Aadhaar has been questionable since it's exceptionally origin. Whenever mooted, the plan was opposed by the home service since confirmation information by UIDAI does not fulfill security criteria. The home service even declined to utilize this information for the National Population Register on the grounds that statutory procedures had not been followed in gathering demographic and biometric information.

The techniques and procedures of information accumulation and capacity for the task may have gotten extreme feedback however they have not got enough investigation. In an as of late composed article I had point by point how the UIDAI has enrolled the administrations of a few private subcontractors, including those that aren't Indian or subject to Indian law for information assemblage, which intensifies the risk to security.

Unless and until there is an extensive enactment on security there is no purpose behind Indian subjects to put their confidence in the great aims of merchants with no specific alliance to our laws. The Central Identities Data Repository, under the UIDAI, is a concentrated database – that is, all demographic and biometric information is put away as one database. This, without an information insurance enactment, is a ticking time bomb. The consequences of focal databases on the protection of nationals are powerful.

The level headed discussion on the privilege to Privacy is just picking up in quality and force universally. Prior this week, the European Court of Justice regarded that the United States Safe Harbor system, which encourages the exchange of individual information from the European Union to servers facilitated in the USA, was insufficient, and held that client information created in the EU will must be represented by EU laws for information security. This now puts the ball in the USA's court, as they will need to coordinate the EU models for protection.

As India inches towards Digital India, it is basic that we too make a vigorous security and information insurance design. In a post-Snowden world, it would be impulsive for us to overlook this. Forgetting about the issue of security is questionable as the administration is not qualified for uphold any state which basically denies a resident of another ensured directly under the Constitution. This “Teaching of Unconstitutional States” rises up out of American Case Laws and was additionally embraced in India through a nine judge seat choice of the Supreme Court in Ahmedabad St. Xavier's College Society v. State of Gujarat<sup>7</sup>, which expressed that, “The principle of “illegal state” implies any stipulation forced upon the award of a legislative benefit which as a result requires the beneficiary of the benefit to give up some protected right.”

### **Evolution of the Right to Privacy**

Preceding going into talks on procurements of the Draft Bill 2011 or the Committee Report, it is intriguing to take a note of the advancement of the privilege to protection under the Indian legitimate administration.

The Supreme Court of India (hereinafter alluded to as the “Preeminent Court”) had the chance to first choose and set out the forms of the privilege to protection in India on account of Kharak Singh v. State of Uttar Pradesh<sup>8</sup>. This case did not witness the acknowledgment of the privilege to protection as a major directly under the 'individual freedom' proviso of Article 21 of the Constitution. Dominant part of the judges for this situation declined to decipher Article 21 in a way to incorporate inside of its ambit the privilege to security, however two of the seven judges declared that the privilege to protection forms a crucial element of individual freedom. In this way, the Supreme Court while choosing the instance of Govind v. State of Madhya Pradesh<sup>9</sup> set out that various central privileges of subjects can be portrayed as adding to one side to protection. In spite of the fact that the Supreme Court likewise expressed that the privilege to security will need to experience a procedure of case by case development. The Supreme Court on account of R. Rajagopal v. State of Tamil Nadu<sup>10</sup> surprisingly straightforwardly connected the privilege to protection to Article 21 of the Constitution and set down:

---

<sup>7</sup> (1974) 1 SCC 717

<sup>8</sup> (1964) SCR (1) 332

<sup>9</sup> AIR 1975 SC 1378

<sup>10</sup> 1994 SCC (6) 632

“The right to security is understood in the privilege to life and freedom ensured to the citizens of this nation by Article 21. It is a “privilege to be not to mention”. A subject has a right to shield the protection of his own, his family, marriage, multiplication, parenthood, tyke bearing and instruction among different matters. None can publish anything concerning the above matters without his assent whether honest or generally and whether commendatory or basic. On the off chance that he does as such, would be violating the right to security of the individual concerned and would be subject in an activity for damages.”

Further, while settling on the issue of phone tapping on account of *PUCL v. Union of India*<sup>11</sup>, the Supreme Court watched that phone tapping would be a genuine intrusion of an individual's privacy. Thus, phone tapping would infract Article 21 of the Constitution, unless it is allowed under the method built up by law.

Accordingly, the idea of protection of an individual has developed throughout the years and has been held to be a basic right by the Supreme Court. On account of *Selvi v. State of Karnataka*<sup>12</sup> the Supreme Court held that an automatic subjection of a man to narco analysis, polygraph examination and BEAP tests damages the privilege to security.

It is to be noticed that even with the extended extent of Article 21 of the Constitution covering right to protection, the privilege to an individual's security is not an outright one and accompanies certain special cases. The Supreme Court watched that the privilege to security might be limited for the counteractive action of wrongdoing, issue or insurance of wellbeing or ethics or assurances of rights and opportunity of other.

The Supreme Court has explained a verifiable right to security got from the dialect set out in Article 21 of the Constitution. Notwithstanding, India does not have a different and particular enactment that expressly perceives the right to privacy and sets out the forms of its pertinence.

The information controller should just gather that individual data from information subjects as is essential for the reasons recognized for such accumulation and additionally handle the information pertinent to the reason for which they are gathered; the information gathered would be put to use for the reason for which it has been gathered. Any adjustment in the use would be done just with assent of the individual concerned; Information gathered and handled would be significant for the reason and no extra information components would be gathered from the person;

Encroachment of any procurement under the Act would constitute an offense for which people may look for remuneration. Indian Aadhaar number appears to be on the same concept provide each and every individual with a unique number as identity. Right to privacy is already

---

<sup>11</sup> (1997) 1 SCC 30

<sup>12</sup> AIR 2010 SC 1974

recognized in USA, phrased as right to be left alone. In United Kingdom and France, laws giving power of collect biometric data were declared unconstitutional.

### **Nilekani's Idea of UID**

The basic concept of having an identity in numerous nations is taken for granted. India tried to attain an advanced and standard identification system for the population since India was lacking a dominant identification system and came out with the idea of Aadhaar to identify each and every individual of the nation. Aadhaar was developed with the objective to tackle the problem of significant problem of introducing the more residents of India into the formal economy, provide greater access to the benefits and preventing country from the embarrassing situation of corruption and malfeasance.

After great deal of efforts and consideration, Nilekani and his team proposed a system where the biometric technology would play the leading role to make sure that, the uniqueness of the identity and prevent the fraud. The proposed technological and institutional infrastructure of Aadhaar was set too high that, it had to be able to eliminate any kind of duplication and faking of identities which were well known in the current and prevalent system in the country.

Nandan Nilekani, expressed himself about his proposition on Aadhaar and his views about Aadhaar were appreciable, as per him, *“The name Aadhaar communicates the fundamental role of the number issued by the UIDAI the number as a universal identity infrastructure, a foundation over which public and private agencies can build services and applications that benefit residents across India.”*<sup>13</sup>

Also the idea of Aadhaar was explained as *“Aadhaar would also be a foundation for the effective enforcement of individual rights. A clear registration and recognition of the individual's identity with the state is necessary to implement their rights –to employment, education, food, etc. The number, by ensuring such registration and recognition of individuals, would help the state deliver these rights.”*<sup>14</sup>

The government through the notification<sup>15</sup> dated 28 January 2009 established an institution named Unique identification Authority of India which was assigned with the task to link each and every single person of the country system by allotting them a unique identity number. Aadhaar project led to the establishment of one of world's largest biometric data system. Aadhaar soon after its introduction became the leading biometric data system of world as they

---

<sup>13</sup>Concept, Unique Identification Authority of India, <http://uidai.gov.in/uid-brand/concept.html>, Last seen June 10, 2016

<sup>14</sup> Ibid

<sup>15</sup>Unique Identification Authority of India, [http://www.uidai.gov.in/images/notification\\_28\\_jan\\_2009.pdf](http://www.uidai.gov.in/images/notification_28_jan_2009.pdf), Last seen June 10, 2016

lead the database of Federal Bureau of Investigation with a huge margin as per the reports released<sup>16</sup>.

Behind the introduction Biometric identity system, the basic idea was clearly mentioned in the notification dated 28 January 2009, but the authority setup through that notification had a great question to answer, and that too regarding legality of the Aadhaar. Well this part of the paper explains the idea of Aadhaar and thus we will discuss its legality in the very next part of the article. However getting back to the objective of the establishment of UIDAI; let's refer back to the notification to discuss the responsibilities which were passed on to UIDAI though the above mentioned notification<sup>17</sup>.

1. Generate and assign UID to the residents. From the very points it is quite clear that, whosoever fulfills that condition given in section 6(1) of income tax act 1961<sup>18</sup>, can apply for the issuance of UID from the authorities.
2. Define mechanisms and processes for interlinking UID with partner databases on a continuous basis.
3. Frame policy and regulate the mechanism of updating of system UIDAI.
4. Define dispute resolution mechanism between involved agencies.
5. Define usage of UID<sup>19</sup>. The usage of UID which has been defined by UIDAI, on being picked from official website of Aadhaar tells that, major banking and financial services are to be connected to UID along with other important services to save the system from

<sup>16</sup><http://aadhaaruid.in/aadhaar-worlds-largest-biometric-id-system-47/>

<sup>17</sup>Notification No. A.03011/02/2009-Admin.I

<sup>18</sup>Section 6 (1), Income Tax Act 1961

For the purposes of this Act,—

(1) An individual is said to be resident in India in any previous year, if he—

(a) is in India in that year for a period or periods amounting in all to one hundred and eighty-two days or more; or

(b) [\* \* \*]

(c) having within the four years preceding that year been in India for a period or periods amounting in all to three hundred and sixty-five days or more, is in India for a period or periods amounting in all to sixty days or more in that year.

[Explanation 1].—In the case of an individual,—

(a) being a citizen of India, who leaves India in any previous year as a member of the crew of an Indian ship as defined in clause (18) of section 3 of the Merchant Shipping Act, 1958 (44 of 1958), or for the purposes of employment outside India, the provisions of sub-clause (c) shall apply in relation to that year as if for the words "sixty days", occurring therein, the words "one hundred and eighty-two days" had been substituted ;

(b) being a citizen of India, or a person of Indian origin within the meaning of Explanation to clause (e) of section 115C, who, being outside India, comes on a visit to India in any previous year, the provisions of sub-clause (c) shall apply in relation to that year as if for the words "sixty days", occurring therein, the words "one hundred and eighty-two days" had been substituted.

[Explanation 2].—For the purposes of this clause, in the case of an individual, being a citizen of India and a member of the crew of a foreign bound ship leaving India, the period or periods of stay in India shall, in respect of such voyage, be determined in the manner and subject to such conditions as may be prescribed.]

<sup>19</sup>*Aadhaar Usage*, Unique Identification Authority of India, <http://uidai.gov.in/aadhaar-usage.html>, Last Seen June 10, 2016

fraud. This move of linking major services with Aadhaar is defaults to the Hon'ble Supreme Court order<sup>20</sup> with regard to UID till the matter gets final.

6. Manage the lifecycle of UID
7. Adopt phased approach for implementation of UID.
8. Take necessary steps to ensure collation of NPR with UID.
9. Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages across partner agencies as well as its validation while cross linking with other designated agencies.
10. Evolve strategy for usage of UID
11. Identify new partner agencies.
12. Issue necessary instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with UID and its partner database.
13. Planning for the resources of UID and taking care of budgeting process of the UIDAI for central unit and all state units.

### Legal issues with the Aadhaar

The big and the basic question which can be put forward with regard to UIDAI is that, how a authority can established without any legislative baking of it. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 was enacted and notified on 26<sup>th</sup> March 2016, which was introduced in the parliament as money bill<sup>21</sup>. The object of the act was to provide, as good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected with it.

Legal existence the authority was challenged in the case of Justice K.S Puttaswamy (Retd.) v. Union of India<sup>22</sup>, through a PIL where, it was contended by the Petitioners that, “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<sup>23</sup>.” It was also contended before the Hon'ble Supreme Court that, “the scheme is unconstitutional as applicants are required to part with personal information on biometrics, iris and fingerprints, infringing their

<sup>20</sup> Writ Petition(s)(Civil) No(s). 494/2012

<sup>21</sup>K. R. Srivats, Aadhaar legislation tabled as a money Bill, The Hindu, <http://www.thehindubusinessline.com/economy/new-aadhaar-bill-introduced-as-money-bill-in-lok-sabha/article8309587.ece>, Last Seen June 10, 2016

<sup>22</sup> Writ Petition(s) (Civil) No(s). 494/2012

<sup>23</sup>J. Venkatesan, Don't tie up benefits to Aadhaar, court tells Centre, The Hindu, <http://www.thehindu.com/todays-paper/tp-national/dont-tie-up-benefits-to-aadhaar-court-tells-centre/article5162837.ece>, Last Seen June 10, 2016

right to privacy, which is held part of the fundamental right to life under Article 21 of the Constitution<sup>24</sup>.” Afterwards it was claimed by the Attorney General that, “The invasion of privacy is of no consequence because privacy is not a fundamental right and has no meaning under Article 21. The right to privacy is not a guaranteed under the constitution, because privacy is not a fundamental right.” To the above mentioned contentions of the parities, court replied that, “The invasion of privacy is of no consequence because privacy is not a fundamental right and has no meaning under Article 21. The right to privacy is not a guaranteed under the constitution, because privacy is not a fundamental right. Privacy telescopes to liberty and the breach of privacy leads to a violation of liberty which is protected under Article 21 of the Constitution.”<sup>25</sup>

Also it was contented by the petitioners that, in this case of data collection ultimate ownership of the data is held by UIDAI and hence they can use it for commercial purpose as well. To this contention, court replied held that, No data shared with UIDAI can be shared with anyone else without consent of the person whose data is to be shared. Court also held that, in case where there is a criminal investigation is pending; sharing of data by UIDAI depends on the order of the court.<sup>26</sup> For further consideration matter has been referred to the constitutional bench of the Supreme Court.

There has been one more instance where the case of sharing of data by UIDAI, where the controversy was brought in the notice of the Superior Court of the country after UIDAI was aggrieved by the order of Bombay High Court. In this case, a girl aged seven years was gang-raped. To crack the investigation, it was court ordered UIDAI to provide the database of all enrolled people to CBI, so that they can check the fingerprints found on the crime scene with the database. Aggrieved by the order of Court, Authority approached Bombay High Court, and contended that database is for civilians use and not to be used as forensic database. But Hon’ble Court recorded that, “the UIDAI had agreed to test the competence of its database in comparing the chance fingerprints with its biometric record and also asked the director general of the Central Forensic Science Laboratory to examine the technological capabilities of the UIDAI database.”<sup>27</sup> This case was later on clubbed with the PIL filled by Justice K.S Puttaswamy (Retd.) v. Union of India<sup>28</sup> and was argued on the ground of Right to Privacy.

### **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016**

After constitution of the authority, legislation was enacted to support Aadhaar in 2016 which was already discriminated all round for various lacunas it carry and its half cooked concept. Though

---

<sup>24</sup> Ibid

<sup>25</sup> Writ Petition(s) (Civil) No(s). 494/2012

<sup>26</sup> Writ Petition(s) (Civil) No(s). 494/2012

<sup>27</sup> Special Leave to Appeal (Crl) No(s).2524/2014 titled Unique Identification Authority of India & another v. Central Bureau of Investigation

<sup>28</sup> Writ Petition(s) (Civil) No(s). 494/2012

object of Aadhaar is already in question along with its constitutionality, legislation was enacted by parliament which got president's assents and got notified on 26 March 2016.

Aadhaar act 2016 has been enacted in to “provide for, as good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith”<sup>29</sup>

Establishment of “Central Identities Data Repository” means a centralized database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto<sup>30</sup> is defined in the Act as a repository of body corporate<sup>31</sup> which will hold all the information of the person enrolled.

Every resident is entitled to get a unique<sup>32</sup>, random<sup>33</sup> and a number acting as proof of identity<sup>34</sup> known to be Aadhaar number, by getting himself enrolled and giving the demographic and biometric information to the authority<sup>35</sup>. And while getting enrolled the person shall be informed about manner of use of information, with whom the information can be shared and authority with whom request to access information can be made<sup>36</sup>.

Aadhaar Act ensures that, special measures are taken while issuance of Aadhaar number to the women,

children, senior citizens, persons with disability, unskilled and unorganized workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and those which are specified in the regulation<sup>37</sup>. Here act does not mention or extend power to any regulation to define what kind of special precautions shall be taken while issuing unique number to categories mentioned in Section 5 of the act 2016. Also, demographic and biometric updation of information may be done Authority from time to time<sup>38</sup>.

To receive benefits given by the state and central government, a person with enrollment of Aadhaar has to go through the process of authentication. Most important thing which is worth

<sup>29</sup> Object of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>30</sup> Section 2(h) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>31</sup> Section 11 (2) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>32</sup> Section 4(1), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>33</sup> Section 4(2), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>34</sup> Section 4(3), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>35</sup> Section 3(1), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>36</sup> Section 3(2), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>37</sup> Section 5 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>38</sup> Section 6 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

mentioning here is that, Aadhaar number does not to confer citizenship or domicile of any person<sup>39</sup>.

Act also confers power to the authority, to hire various entities to maintain the data repository<sup>40</sup>. This is where the concerns rises as, authorities may hire a number of private entities to collect data for them and which questions the privacy of the people enrolled for the unique number.

Act establishes a body corporate authority to regulate the functions of the as issuance of number and maintenance of data. This authority shall have a chairperson which may be on part-time basis or full time basis, two part time members and a CEO who will act as a member secretary of the authority. Term in office of the chairman and members shall be three years or till 65 years of age<sup>41</sup>.

Section 23 of the act expressly provide for the regulating power of the Authority and mentions instances where, the authority may frame regulations to control the functions and use of Aadhaar number. "The Authority shall develop the policy, procedure and systems for issuing Aadhaar numbers to individuals and perform authentication

- (a) Specifying, by regulations, demographic information and biometric information required for enrolment and the processes for collection and verification thereof;
- (b) Collecting demographic information and biometric information from any individual seeking an Aadhaar number in such manner as may be specified by regulations;
- (c) Appointing of one or more entities to operate the Central Identities Data Repository;
- (d) Generating and assigning Aadhaar numbers to individuals;
- (e) Performing authentication of Aadhaar numbers;
- (f) Maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;
- (g) Omitting and deactivating of an Aadhaar number and information relating thereto in such manner as may be specified by regulations;
- (h) Specifying the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used;
- (i) Specifying, by regulations, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof;

<sup>39</sup> Section 9 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>40</sup> Section 10 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>41</sup> Section 11 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

- (j) Establishing, operating and maintaining of the Central Identities Data Repository;
- (k) Sharing, in such manner as may be specified by regulations, the information of Aadhaar number holders, subject to the provisions of this Act;
- (l) Calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of this Act of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act;
- (m) Specifying, by regulations, various processes relating to data management, security protocols and other technology safeguards under this Act;
- (n) Specifying, by regulations, the conditions and procedures for issuance of new Aadhaar number to existing Aadhaar number holder;
- (o) Levying and collecting the fees or authorizing the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act in such manner as may be specified by regulations;
- (p) Appointing such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act;
- (q) Promoting research and development for advancement in biometrics and related areas, including usage of Aadhaar numbers through appropriate mechanisms;
- (r) Evolving of, and specifying, by regulations, policies and practices for Registrars, enrolling agencies and other service providers;
- (s) Setting up facilitation centers and grievance redressal mechanism for grievances of individuals, Registrars, enrolling agencies and other service providers;
- (t) Such other powers and functions as the act of 2016 may prescribe.<sup>42</sup>

Act promises to take all necessary and relevant steps to maintain safety of the data collected<sup>43</sup>. Biometric information such as an individual's finger print, iris scan and other biological attributes (specified by regulations) will be used only for Aadhaar enrolment and authentication, and for no other purpose. Such information will not be shared with anyone, nor will it be displayed publicly, except for purposes specified by regulations<sup>44</sup>.

The information of the person may be revealed in two cases only<sup>45</sup>,

---

<sup>42</sup> Section 23 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>43</sup> Section 28 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>44</sup> Section 29 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>45</sup> Section 33 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

(a). In the interest of national security, a Joint Secretary in the central government may issue a direction for revealing, (i) Aadhaar number, (ii) biometric information (iris scan, finger print and other biological attributes specified by regulations), (iii) demographic information, and (iv) photograph. Such a decision will be reviewed by an Oversight Committee (comprising Cabinet Secretary, Secretaries of Legal Affairs and Electronics and Information Technology) and will be valid for six months.

(b) On the order of a court, (i) an individual's Aadhaar number, (ii) photograph, and (iii) demographic information, may be revealed

A person may be punished with imprisonment up to three years and minimum fine of Rs 10 lakh for unauthorized access to the centralized data-base, including revealing any information stored in it. If a requesting entity and an enrolling agency fail to comply with rules, they shall be punished with imprisonment up to one year or a fine up to Rs 10,000 or Rs one lakh or both under the provisions of this act. Also, No court shall take cognizance of any offence except on a complaint made by the UID authority or a person authorized by it.<sup>46</sup>

### Challenges

First of all, it is worth mentioning that, Government introduced Aadhaar Bill as a money bill under Article 110<sup>47</sup> of the Constitution of India. So that, role of Rajya Sabha can be limited and thus, bill discussion if even happen in Rajya Sabha and they find it unworthy to be passed does not hamper its chances to get passed. This act of the government can be termed as the mockery of the Constitutional process.

Article 110 limits a 'money bill' only to six specific instances: covering tax, the government's financial obligations and, receipts and payments to and from the Consolidated Fund of India, and, connected matters. The abovementioned act lies well outside the scope of the said article and hence validity of act may be questioned in the court on this ground as well.

One of the biggest challenges is that, Aadhaar is under the scanner of Supreme Court because; it has been claimed by various that it Aadhaar will violate right to privacy of the people enrolled herein. Some of the complications of the Act are discussed hereunder:

- Act is silent regarding consent being acquired in case of the enrolling agency or registrars. However, section 8 provides that any requesting entity will take consent from the individual before collecting his/her Aadhaar information for authentication purposes, though it does not specify the nature<sup>48</sup>.

---

<sup>46</sup> Section 47 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>47</sup> Article 110 of the constitution of India 1950

<sup>48</sup> <http://cis-india.org/internet-governance/blog/aadhaar-act-and-its-non-compliance-with-data-protection-law-in-india>

- Section 3 of the Act states that at the time of enrolment and collection of information, the enrolling agency shall notify the individual as to how their information will be used; what type of entities the information will be shared with; and that they have a right to see their information and also tell them how they can see their information. However, the Act is silent regarding notice of name and address of the agency collecting and retaining the information<sup>49</sup>.
- The Aadhaar Act does not provide an opt- out provision and also does not provide an option to withdraw consent at any point of time. Section 7 of the Aadhaar Act actually implies that once the Central or State government makes Aadhaar authentication mandatory for receiving a benefit then the individual has no other option but to apply for an Aadhaar number. The only concession that is made is that if an Aadhaar number is not assigned to an individual then s/he would be offered some alternative viable means of identification for receiving the benefit. Government is very rashly moving to that step when they will declare Aadhaar mandatory to avail benefits of social security scheme. However this step of central government timely went in under the scanner of Supreme Court<sup>50</sup>.
- Section 28 of the Act states that the UIDAI must ensure the security and confidentiality of identity information and authentication records. It also states that the Authority shall adopt and implement appropriate technical and organizational security measures, and ensure the same are imposed through agreements/arrangements with its agents, consultants, advisors or other persons. However, it does not mention which standards/measures have to be adopted by all the actors in Aadhaar ecosystem for ensuring the security of information, though it can be argued that if the contractors employed by the UIDAI are body corporate then the standards prescribed under the IT Rules would be applicable to them.

## Conclusion

India is one of the first countries in the world that has initiated a biometric identification system for all residents<sup>51</sup>. Introduction of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 has provided much controversial, disputed but quite fancy and unique program of Nandan Nilekani not only legal backing but also new life to the most anticipated project of recognizing each and every resident with a unique number. Well this new act of 2016 intends to connect all the financial and subsidized benefits as well as the banking to the Aadhaar number. Identity theft may not be possible from biometric data but, collection of data is done by the hired private entities and there is nothing in this act to deal with the issue of

---

<sup>49</sup> Ibid

<sup>50</sup> Ibid

<sup>51</sup> Praveen Kumar and Chander Kant, *Unique Identification System In India: A Big Challenge*, Vol. 5, International Journal of Information Technology and Knowledge Management, pp. 447-451, 2012, <http://www.serialsjournals.com/serialjournalmanager/pdf/1346060261.pdf>, Last Seen June 10, 2016

misuse of data collected thereto. Also UIDAI, data repository has to be very cautious from the hackers, as hacking may result in the loss of valuable data of the public. If data gets in wrong hand will prove very costly to the economy of the country for sure. Penalties are not enough to tackle data tempering.

The success or failure of the Aadhaar project remains to be determined. Even though the detailed analysis focused on biometric identification system in India, the practical application and findings of the public-private partnership can be applied in a broader perspective. Whether Aadhaar is successful or not, the outcomes and implications will be a notable indication for other nations to determine if the application of a biometric identification system should be adopted in the interests of their own residents.