Xournals

Academic Journal of Law and Judiciary

ISSN UA | Volume 01 | Issue 01 | January-2019

Aadhaar- The Basis of an Indian

Yogesh Chalisa[1]

Available online at: www.xournals.com

Received 7th September 2018 | Revised 10th October 2018 | Accepted 13th December 2018

Abstract:

From the origin in 2009, the Aadhaar project has been covered in argument because of the different questions are raised about the technological issues, privacy, welfare prohibiting, and security concerns. The project is ladled with serious lacunae and it lacks security of the personal identity information, openness in the working of the UIDAI, proper supervision, redress mechanisms and accountability. Legal framework is sketchy and not adequate. But on the other hand, succeeded in removing the bottlenecks from the government subsidy delivery chain, making of the passport, opening bank accounts, disbursing pensions, provident fund and thereby it saved a lot of money of the government. The World Bank is so impressed with the aadhaar that it recommended other countries to in the world to adopt it Countries like Bangladesh, Tanzania, Russia, Afghanistan, Morocco, Tunisia and Algeria have conveyed concern in the system. Government asserted Supreme Court, by linking Aadhar to PAN card for removing the fake PAN card which are used for terror backing, drug financing, and exchange of black money that is almost all the major problems country is facing today. Now it becomes so ambitious that it is now not considered less than messiah. The aadhaar project has been depicted not only as a new face of development that technology could bring about but also as an identity technology that will open us all up to discrimination, prejudice, the risk of identity theft any subject the entire population of the country under continuous surveillance. There are reports claiming that the aadhar is saving over 1 billion dollar of the government. There are also reports that nearly 135 aadhaar numbers and some personal information has been disclosed. Therefore this project has both positive as well as negative aspect. This paper is intended to examine both these aspects and to reach at the conclusion with a suggestion how these problems can be solved.

Key Words: *Aadhaar- The Basis of an Indian*

Authors:

1. *K.H. Government Degree College, Anantapur, Andhra Pradesh, INDIA*

INTRODUCTION

With the aim of weeding out corruption and personification from government service and welfare supply chain, the aadhaar project was launched in 2009. Under this project, a random and unique number, which can singularly identify people, is generated using some biometric (fingerprint, photograph, scaning of iris etc.) and personal information (name, address, birth date etc.) of the people. National Identification Authority of India Bill, 2010 (hereinafter as the NIAI Bill) was came into existence in the Loksabha to give statutory back-up to the project. Standing Committee on Finance of the 15th Loksabha, however, rejected it and observed that "the scheme is ladled with serious lacunae and representation of legislature of a data security and confidentiality is an essential for the Aadhaar system." But the project was continued to be executed without any legislation. A new bill, Aadhaar (Directed Transfer of Financial and Other Grants, Welfares and Facilities) Bill, 2016 (after Aadhaar Act, 2016) finally get passed. But this bill got criticized for not accepting five recommendation of Rajya Sabha, for absence of any opt-out option, for no effective and comprehensive provisions pertaining to cybersecurity of Aadhaar, for no safeguards for the privacy of the personal identity information, for no limitation over-collection of information for the registration under the scheme, for disclosure of the personal information by the requesting agency under section 8, for disclosure of the aadhaar information, for undefined national security under section 33, for no prescription of data-breach notification, for striping legitimate citizens of their right to report criminal activities and breaches concerning Aadhaar, for involvement of private entity in the upkeep and formation of the CIDR under Section 10, for the composition of oversight committee to check misuse of disclosure of aadhaar information prescribed under section 33 and for over delegation of power to Unique Identification Authority of India (hereinafter as the UIDAI). Parliament in contrast to the aadhaar act and the temporary order of Supreme Court passé August 11 and October 15, 2015, made an amendment and inserted Section 139AA in the Income Tax Act, in which aadhaar was made compulsory to fill the income tax proceeds and PAN number with effect from 1 July 2017. This amendment too shrouded aadhaar in controversies because it allegedly violates right of informational self-determination[1].

However, this project succeeded in removing the bottlenecks from the government subsidy delivery chain. Making of the passport, opening bank accounts, disbursing pensions and the provident fund now become easier and faster. The World Bank is so impressed with the aadhaar that it recommended other countries to in the world to adopt it.[2] This project also received global acclaim from entities like Bill Gates, *The Economist*, the World Bank, Raoul Pal, and others. Countries like Bangladesh, Tanzania, Russia, Afghanistan, Morocco, Tunisia and Algeria have conveyed concern in the system[3]. Government, reportedly, per year saves approximately USD 1 billion (Rs 650 crores) transfer cost below Mahatma Gandhi National Rural Employment Guarantee Act, supplying of LPG subsidy, and disbursement of pension, provident fund and ration under PDS scheme. The government asserted Supreme Court, the linkage of Aadhaar with the PAN card will help to remove the fake PAN cards which are used for terror backing, drug financing, and exchange of black money that is almost all the major problems country is facing today.[4] Now it becomes so ambitious that it is now not considered less than Messiah. Therefore this project has positive

[1] A proposition developed by the Federal Constitutional Court of Germany in a ruling relating to personal information collected during that country's 1983 census.

[2] Jeanette Rodrigues, Aadhaar wins, World Bank praise amid 'big brother' fears, Live Mint (Mar 16, 2017, 08:30 IST), http://www.livemint.com/Politics/Y0WwNHySlbDKDFMMvw57nM/Aadhaar-wins-World-Bank-praise-amid-big-brother-fears.html.

[3] World Bank thinks Aadhaar System in India is very effective and should be adopted by all nations (Mar. 17, 2017), https://yourstory.com/2017/03/aadhaar-system-world-bank/.

[4] Other than stopping people from wearing a helmet in their hands, Aahaar can fix every other problem: Govt to SC (May 07, 2017), http://www.fakingnews.firstpost.com/india/stopping-people-wearing-helmet-hands-aadhaar-govt-sc-20776.

as well as negative aspects. It will not be right to abandon this project merely for these lacunae but this also equally not right to not do anything to improve the current on-going project. This paper is intended to evaluate and examine both the negative and positive points of the project and reaching the conclusion with the mid-way solution.

Achievements of Aadhaar

Aadhaar (English translation "the basis") as the names suggest, is an essential and single most important document for identification purposes and KYC verification. Aadhaar succeeded in removing the bottlenecks from the government subsidy delivery chain, making of the passport, opening bank accounts, disbursing pensions, provident fund and thereby it saved a lot of money of the government. The World Bank is so impressed with the aadhaar that it recommended other countries to in the world to adopt it.[5] Countries like Bangladesh, Tanzania, Russia Afghanistan, Morocco, Tunisia and Algeria have stated concern in the system[6]. Taking inspiration from 3 schemes benefits from the aadhaar has been widened. Now it becomes so ambitious that it is now not considered less than the messiah. Recently Government asserted Supreme Court, by linking Aadhar with PAN card can be able to extract out the fake PAN cards which are used for terror backing, drug financing, and movement of black money that is almost all the major problems country is facing today.[7] Biometric identification has so much influenced the government that it has proposed in the Supreme Court the similar unique identification system for the cows too to keep track cows and prevent their smuggling. This section tries to enlist some of those achievements.

Direct Bank Transfer

For Direct Bank Transfer (DBT), 12 digits identification numbers of Aadhaar card is used for person benefits under social wellbeing plans was made to stop replica candidates, scams, and middleman and stop corruption in government. It is now being used to get LPG subsidy, availing of other subsidies without registration and enrollment for getting these individually, monthly pension, provident fund and scholarships for the students directly in the bank account. This refutes the chances of the funds being embezzled or of persons building fake assertions in order to claim profits. Since 2013, through the use of DBT, growing amount of Rs 17869475 has been transferred for 138 schemes under 27 ministries. 29 several economic outlines like Aadhaar Payments Bridge (hereinafter referred as APB) and Aadhaar Enabled Payment Systems (hereinafter referred as AePS) have been constructed by National Payment Corporation of India to backing DBT and also to permit persons use Aadhaar for expenses. In the PDS scheme alone almost Rs 14,000 crore has been saved.[8]

Universal Identification-

The Aadhaar card is a general card which does not any specific purpose unlike the voter ID which is used to participate in the electoral process. In spite of having specific purpose, aadhaar card is used for many purposes like identity proof, age proof as well as address proof. It is universally acceptable card issued by the government, without requiring to

[5] Jeanette Rodrigues, Aadhaar wins, World Bank praise amid 'big brother' fears, Live Mint (Mar 16, 2017, 08:30 IST), http://www.livemint.com/Politics/Y0WwNHySlbDKDFMMvw57nM/Aadhaar-wins-World-Bank-praise-amid-big-brother-fears.html.

[6] World Bank thinks Aadhaar System in India is very effective and should be adopted by all nations (Mar. 17, 2017), https://yourstory.com/2017/03/aadhaar-system-world-bank/.

[7] Other than stopping people from wearing a helmet in their hands, Aahaar can fix every other problem: Govt to SC (May 07, 2017), http://www.fakingnews.firstpost.com/india/stopping-people-wearing-helmet-hands-aadhaar-govt-sc-20776.

[8] Linking Aadhaar to ration cards saved Rs 14000 crore: Ram Vilas Paswan, The Economic Times (May 04, 2017, 10:12 PM IST), retrieved from http://www.business-standard.com/article/economy-policy/linking-aadhaar-to-ration-cards-saved-rs-14-000-cr-ram-vilas-paswan-117050401349_1.html

register or put on for a distinct card for each of these amenities.

Ease of Availability:

The Aadhaar card is issued by the government and considered as the government document which is present at each person and everywhere. For making the aadhaar card, online facilities is available in which aadhaar card present in electronic form called e-aadhaar. This e-aadhaar can be downloaded and person is able to access anytime at anywhere whenever or wherever required. Through the Aadhaar card, individuals are able to have the copy of any government document in the form of identity proof. And it is easily accessible. The copying form and e-aadhaar card reduce the risk of stealing or misplaced the documents because it can be downloaded from any device and displayed when needed.

Digital Life Certificate

For obtaining the pension without their physical presence, the 'Jeevan Praman for Pensioners' or the Digital Life Certificate was introduced by Electronics and IT Department for the persistence of their arrangement. Pensioners can now benefit pension without going outside from their homes because the details are accessible by the department with the help of their Aadhaar Card numbers.

Digital Locker:

For securing the personal document on server of government, the Indian government has launched a digital locker (DigiLocker) system for everyone. For signing up at the server, there is need of 12 digit aadhaar card number of person.

Voter Card Linking:

On 9th March 2015, Aadhaar card UIDAI number was connected to the voter Ids. This act is taken to exclude fake voters. Once an Aadhaar number is connected, it would become difficult for those persons who have multiple voter ID card for illegal purpose, as registering needs voter card holder to be bodily present and gather Aadhaar card to the voting booth officer for connecting.

Removed bottlenecks from the bureaucracy

By using Aadhaar Card, passports can be attained by candidates within 10 days. The persons who wants to obtain a passport can request online by attaching their aadhaar card simply as the identity proof and residence address with the application. Economic institutes and banks believed that Aadhaar Cards is a valid identity and address proof for opening an account in bank. The Aadhaar card is used for KYC, documentation and confirmation purposes. Basic banking or "no-frills account" are being issued by the banks under Jan Dhan Yojna in which individuals can receive the benefits from government strategy through the use of Aadhaar as the primary authentication.[9] For the refugee people in cities, who survive in shantytowns or illegal bunches and have unstable homes, any job asked for the identity proof. For opening the account in bank, gas connection or even request for a ration card – was continually an issue. For resovling these problem, Aadhaar card is used as an identity proof whenever they moved or shift.

Controversies surrounding the Aadhaar and their analysis

From the beginning in 2009, the Aadhaar scheme has been covered in argument because of numerous problems raised like technological issues, confidentiality, well-being prohibiting, and safety worries.[10] In this section, those controversies will be thoroughly analysed.

Right to privacy under the Aadhaar project

The Aadhaar project is revolutionary and groundbreaking. It plunged leakages in the government benefits and subsidy supply chain. But it is not only these positive points that made it so

[9] NPCI. Frequently Asked Questions By Banks for Aadhaar Enabled Payment System, National Payments Corporation of India, http://www.npci.org.in/documents/AEPSFAQBank.pdf.

[10] Information security practices of aadhaar or lack thereof a documentation of the public availability of aadhaar numbers with sensitive personal financial information (May 01. 2017), http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

famous. The suspected threat to the right to privacy pose by it is a contributory element in its popularity. And this threat to the right to privacy was one of the reasons that made a governmental upright group, which led through Yashwant Sinha to reject National Identification Authority of India Bill, (hereinafter referred as the NIAI Bill) in 2011. Following the rejection of the bill, the aadhaar project continued to be executed without any statutory back up until Aadhaar (Directed Transfer of Financial and other Grants, welfares and amenities) Act (after as the aadhaar Act) was passed in 2016. This act has following sections and provisions that allegedly pose threat over the right to privacy.

Section 8 made the identity information openly accessible

According to Section 8 of the aadhaar act, the person who pay the fees, is asked for the identity infomrtaion like photographs, but not nay biometric information to be shared during authentication provided the requesting entity must inform the Aadhaar card holder about the use it offers to make of individuality data and it cannot publish or display the Aadhaar number.

This section lacks any tangible safeguards to prevent any misuse of the data by the requesting agency and important identity information is rendered to be openly accessible. For instance, before buying sim card using aadhaar, it would be unpractical to expect from any person to read the well pattern of the terms and circumstances, or before clacking "I agree" when connecting novel software. And after taking nominal consent by this way there is nothing that can prevent a requesting entity from sharing the identity data like name, birth date, address, or even photograph.[11]

Involvement of the private players in the registration for and generation of the Aadhar numbers

Enrollment of individuals for Aadhaar, as per the aadhaar act, is done by the public and government sector agencies is called the registrars. They can appoint enrolment organizations which plays as a private players who gather demographic and biometric data. These private players are allowed to hire enrollment supervisors and operators by the help of third parties. The aadhaar act lacks any provision for a secure system in place to protect contrary to the breach of information from any of these facts or to guarantee that enrolment organizations and workers do not retain a copy of the record when they transfer it to the administration. There are some instances reported when enrolment organizations and workers handle the data, accessible to them, in a chance mode.[12]

Disclosure of the aadhaar numbers

Different information is collected by numerous agencies in the nation for the purpose of statistics authorized by the Collection of Statistics Act, 2008.[13] By publishing a notification in the official Gazette, the information is gathered and Section 9(4) bans the publication of recognizing information unless allowable by the concerned individual. In the same way, the publication of Aadhaar numbers is also banned according to the Section 29 (4) of the Aadhaar Act, 2016 unless the consent to print them is required from the Aadhaar number container. But recent events have proven that Aadhaar numbers can be easily disclosed, posted online and used for malicious purposes. On May 1, researchers at the Internet and Society Center in Bangalore reported, about 135million Aadhaar numbers had been disclosed online from four distinct government records.[14] There are different type sof database in

[11] Jean Dreze, Hello aadhaar goodbye privacy (Mar. 24, 2017), https://thewire.in/118655/hello-aadhaar-goodbye-privacy/

[12] Usha Ramanathan, Who Owns the UID Database? Medianama (May 6, 2013), http://www.medianama.com/2013/05/223-who-owns-the-uid-database-usha-ramanathan/.

[13] PRS India. (n.d.). The Collection of Statistics Act, 2008, PRS India (Jan. 09, 2009), http://www.prsindia.org/uploads/media/vikas_doc/docs/1241607771~~The%20Collection%20Of%20Statistics%20Act,%202008.pdf.

[14] Rohith Jyothish, Aadhaar vs security: is the biometric system a tool for surveillance? (May 6, 2017, 12:27 PM), http://www.business-standard.com/article/economy-policy/aadhaar-vs-security-is-the-biometric-system-a-tool-for-surveillance-117050600183_1.html

which first two are connected to the rural development ministry. These two are; National Rural Employment Guarantee Act (NREGA) portal and National Social Assistance Programme (NSAP) dashboard. While the other two inbuilt with Andhra Pradesh that is state have their own NREGA portal and online dashboard of a government scheme known as Chandranna Bima. The type of data disclosed included names, names of parents, PAN numbers, mobile numbers, religions, marks, the status of Aadhaar applications, and beneficiaries of welfare schemes, bank account numbers, IFSC codes and other sensitive information. The most famous was the leak of Mahendra Singh Dhoni's aadhaar application form. The report claims these government dashboards and databases revealed personally identifiable information (PII) due to a lack of proper controls exercised by the departments.[15] Most of these reports refer to publications of individually recognizable data of beneficiaries or topics of the records comprising Aadhaar numbers of persons sideways with extra individual identifiers. All of these revelations are indicative of an important and possibly permanent confidentiality damage.[16] The privacy risk is huge in this cases because the simple combination of a person's name, phone number and bank account number is sufficient for numerous cyber-attacks such as phishing.[17] However, Ministry of Electronics and Information Technology dated 25 March 2017 direct state and central department to not to publish this aadhaar and other identity information online and to remove the information that is already published online.[18]

Implications of Disclosure

The initiatives by the government open data portals NREGA, NSAP, Andhra Pradesh NREGA portal and the online dash of an administration system called "Chandranna Bima" can be admirable for offering simple access to administration information shortened for easy breakdown, though in the deficiency of appropriate controls trained by the administration sections inhabiting the records which update the data on the dashes, by revealing the sensitive and private information of an individual who are the answering unit of the databases, the outcomes may be terrible.[19] Through aadhaar number and some basic identity information, other grainy information regarding the individuals containing delicate PII like religion, caste, address, photos and credit card number, details of bank account, and passwords can easily be retrieved over social production to steal currency from the account of an individual.[20] The prime example as the call is received by individuals and claims, calling from bank.[21] Another method is changing the phone number linked to aadhaar number maliciously. There are also some brokers which buy tonnes of duplicates of Aadhaar forms from workshops vending SIM cards and other institutes, with the intention of identity fraud.[22] In the current past, it has been described cases of employees of facilities supplier trapped thieving the biometric data gathered for

[15] Govt may have made 135 million Aadhaar numbers public: CIS report (May 02, 2017, 04:43 AM IST), http://www.livemint.com/Politics/oj7ky556p6vdljXpRw8gPP/135-million-Aadhaar-numbers-made-public-by-government-author.html?li_source=LI&li_medium=news_rec

[16] Information security practices of aadhaar or lack thereof a documentation of the public availability of aadhaar numbers with sensitive personal financial information (May 01. 2017), http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

[17] Asheeta Regidi, GOI directs removal of Aadhaar info published online, what the law says and what to do if your find your data online first post (Mar. 30 2017, 07:21 PM IST), http://www.firstpost.com/india/goi-directs-removal-of-aadhaar-info-published-online-what-the-law-says-and-what-to-do-if-you-find-your-data-online-3360372.html.

[18] Ibid.

[19] Gordon, P. Data Leakage - Threats and Mitigation, 2007, October 15, https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931.

[20] Social engineering fraud, from Interpol: https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud.

[21] Information security practices of aadhaar or lack thereof a documentation of the public availability of aadhaar numbers with sensitive personal financial information (May 01. 2017), http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1.

[22]Reddy, L. V. Hyderabad: Note cheats use Aadhaar card copies, Deccan Chronicle (Nov. 17, 2016), http://www.deccanchronicle.com/nation/current-affairs/171116/hyderabad-note-cheats-use-aadhaar-card-copies.html.

Aadhaar authentication.[23] The government stated that approximately 34000 machines have been banned which were creating the fake Aadhaar numbers.[24] Even biometric data can be collected, for instance taking the iris data of an individual with high resolution with direction camera at a distance, lifting of fingerprints through remote.[25] There are many factors which give the opportunity for the financial fraud in which details if DBT transfers, public presence of Aadhaar numbers, seeded bank account numbers, and registered mobile phone numbers are included. In the US, the receiving of the Social Security Numbers from public records is very easy that caused in many cases of identity theft.[26] These threats increase multifold in India due to the charting of the aadhaar number with bank accounts under Aadhaar enable Payments System (AePs) and Aadhaar Payment Bridge (AePS).[27]

By the AePS, there is a case where the financial fraud took place but the consumer was not able to make his claim for the compensation because of the terms and conditions regarding liabilities. Due to the terms, the consumer took liabilities on oneself rather than the fee provider. The terms and circumstances have been unclear in the current AePS requests like BHIM Aadhaar App.[28] Guidelines and principles round Aadhaar are at a very early and budding phase producing a growth in economic risk for both customers and banks to endeavor into AePS.[29]

Over delegation of powers to the UIDAI

The rules formed by the UIDAI having some matters which are as follows:

The procedure for collecting the information, and its verification, information access, Sharing and revelation of information, Change in information, Appeal and reply for authentication, Important of Aadhaar numbers, confidentiality and safety processes, Identifying procedures connecting to data administration, security procedures and other knowledge protections under this Act and Creating protest redressal apparatuses.

This Act allows the policymaking a very high degree of optional control. A number of significant powers which should preferably be in the purview of the government are substitute to the UIDAI. The UIDAI has been managing the plan since its beginning, and a number of issues have now been acknowledged in the course such as gathering, confirmation, distribution of information, confidentiality and safety courses. Rather than showing these issues, the Act permits the UIDAI to remain to have similar controls. Even the control to set up such a device is surrogate to the UIDAI under Section 23 (2) (s) of the Act in spite of the fact that building the thing managing a plan, also accountable for giving the frameworks to show the complaints rising from the plan, harshly negotiations the individuality of the complaint redressal build.

[23] Singh, S. R. RJio SIM cards being sold on the black market in Delhi, Business Line (Sep. 22, 2016), http://www.thehindubusinessline.com/info-tech/rjio-sim-cards-being-sold-in-the-black-market-in-delhi/article9136775.ece.

[24] PTI. Govt asserts no poor will be deprived by making Aadhaar mandatory, Hindustan Times (April 10, 2017), http://www.hindustantimes.com/india-news/govt-asserts-no-poor-will-be-deprived-by-making-aadhaar-mandatory/story-G2OBbLDaGFuYISwUqHJ8pL.html.

[25] Agrawal, S., Banerjee, S., & Sharma, S. (n.d.). Privacy and Security of Aadhaar: A Computer Science Perspective, from IIT Madras, http://www.cse.iitm.ac.in/~shwetaag/papers/aadhaar.pdf.

[26] The Identity Project, London School of Economics, http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf.

[27] Joe C Mathew, Aadhaar must up security measures to ward off financial frauds, says the report, Business Today (May 11, 2017, 04:01 PM IST), http://www.businesstoday.in/current/economy-politics/aadhaar-must-up-security-measures-to-ward-off-financial-frauds-says-report/story/251403.html.

[28] Menon, S. Are the terms and conditions of BHIM-Aadhaar anti-consumer or simply anti-interpretation?, Newslaundry (April 20, 2017), https://www.newslaundry.com/2017/04/20/are-the-terms-and-conditions-of-bhim-aadhaar-anti-consumer-or-simply-anti-interpretation.

[29] Information security practices of aadhaar or lack thereof a documentation of the public availability of aadhaar numbers with sensitive personal financial information (May 01. 2017), http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

No Effective Provisions for Cybersecurity

The demographic and biometric data of peoples gathered under the Act is kept in a central record called 'Central Identities Data Repository' (CIDR), which is under the regulation of Unique Identification Authority of India (UIDAI).

The Aadhaar (Targeted Delivery of Financial and Other Grants, Welfares and Amenities) Act, 2016 (after referred to as the Aadhaar Act, 2016) was passed to grant legality to Aadhaar. However, the Aadhaar Act, 2016 did not address all relevant and imperative issues concerning Aadhaar in a comprehensive manner.

We need to appreciate that security is critical for the further success of the Aadhaar ecosystem. When one looks at the provisions of the Aadhaar Act 2016, one finds that no effective and comprehensive provisions pertaining to cybersecurity of Aadhaar ecosystem are incorporated under the Aadhaar Act, 2016.

The Aadhaar Act, 2016 has itself been drafted keeping in mind just the safety of identity data and verification accounts of persons kept in the Central Identities Data Repository.

The very fact that the Aadhaar Act, 2016 has not done enough for cyber security has ensured that the breaches will continue.

Given the resolve of the government to make Aadhaar mandatory, it needs to look at a broader vision of trying to make the Aadhaar ecosystem more cyber secure, rather than just the narrow vision of protecting the security of the Central Identities Data Repository.

Voluntary v Mandatory

Using biometrics of a person for identification to get rid of fraud and duplication is a very effective idea. But there is also another aspect of this. Biometrics of any person are core to his/her identity and every individual has a right of "informational self-determination". Therefore biometrics of any person can't be taken apart from him forcefully from him for whatsoever reason.[30]. An individual must be allowed to determine what information of his can be allowed to be put out and this is closely tied to a person's right to dignity.[31] The state has no eminent domain in making a law that forces a citizen to part with biometrics.[32] Taking cognizance of bodily interest and personal interest of individuals, on August 11 and October 15, 2015, Supreme Court stated in unmistakable relations, that Aadhaar could not be compulsory, and but it can be used for the 6 purposes detailed by the government earlier it. "The Aadhar Act itself envisages free consent.[33] But the Aadhaar slowly became compulsory for a wide variety of services through various administrative orders in spite of the Supreme Court stating that the Aadhaar card should not be compulsory. Looking for the agreement for connecting the Aadhaar number with the bank account does not have meaning only bank demand for the aadhar card number from customers. On the other side, income tax also demand for the aadhaar card number from assessment year. The advertisements are made by Election Commission in which they asked people to link their election identity cards with the aadhaar card. In Delhi, even witnesses to property-related transactions registered in courts have to provide their Aadhaar numbers. To avail benefits of the scholarships, student has to have their Aadhaar identification number.[34] Now

[30] A proposition developed by the Federal Constitutional Court of Germany in a ruling relating to personal information collected during that country's 1983 census.

[31] Advocate Shyam Divan makes a case against govt rulemaking Aadhaar must file tax returns, Live Mint (Apr. 29, 2017, 12:29 AM), http://www.livemint.com/Politics/snjp639veqmeanRxdjE22J/Advocate-Shyam-Divan-makes-case-against-govt-rule-making-Aad.html.

[32] Shyam Divan concludes arguments in Aadhaar case in Supreme Court, Live Mint (Apr. 28, 2017, 04:15 PM IST), http://www.livemint.com/Politics/sN0S5mYYx641tgrctGf03H/Shyam-Divan-concludes-arguments-in-Aadhaar-case-in-Supreme-C.html.

[33] PTI, ***Alive to early orders that aadhaar should be voluntary,*** The New Indian Express (Apr. 28, 2017, 02:23 AM IST), http://www.newindianexpress.com/nation/2017/apr/28/alive-to-earlier-orders-that-aadhaar-should-be-voluntary-sc-1598687.html.

[34] Live Law, Why Is Aadhaar card mandatory for availing of Minority Student's Scholarships: Delhi HC asks Centre, Live Law (Sept. 7, 2016, 05: 41), http://www.livelaw.in/aadhar-card-mandatory-availing-minority-students-scholarships-delhi-hc-asks-centre/.

parliament also made an amendment and inserted Section 139AA of the Income Tax Act which gives the compulsory points of Aadhar or enrolment ID of Aadhar application form to fill the income tax returns and creating request for provision of PAN number with outcome from 1 July this year. The parliament did so, surprisingly, without amending the aadhaar act.

By no means, the author wanted to challenge the authority and prudence of the parliament. The SC's 2015 order was mandamus only to the government, which was executed and it cannot be a mandamus against Parliament".[35] And if parliament wanted to make aadhaar mandatory then they could do it. The parliament change the 30 judgment of the Supreme Court but in earlier cases, parliament took precaution for changing the basis of a judgment before overruling it. In this case also if the government wants to make aadhaar mandatory then it must amend the Aadhaar Act to make it compulsory for all purposes. But it is surprising that Parliament, which had passed the Aadhar Act last year as voluntary, has enacted section 139AA which makes it mandatory[36]. Section 139AA of the Income Tax Act creating Aadhaar compulsory to fill the income tax returns is contrary to the Aadhaar Act. [37]

The difference between the aadhaar act and various government decisions which made aadhaar mandatory necessary for availing government benefits created a lot of muddle about the Aadhaar card whether it is charitable or compulsory and whether the deficiency of it can be used to refute somebody a facility. As per this information, the fact that it will become only point of entrée to information about all regarding a separate, which is why the confidentiality matter is supreme?

Surveillance

Under the aadhaar Act, the most contentious topic of safety and confidentiality of individuals' electronic data is dealt in the Protection of Information's Chapter VI. In Clause 30, demographic and biometric information is considered as *"electronic record,"* and *"sensitive personal information or data"* as stated in the Information Technology Act, 2000. If any individual or company imitates, deliberately reveals, conveys, reproductions or distributes, harms, steals, hides, abolishes, erases or changes, or interferes with etc. such energetic data, it is to be observed as an crime which is explained in Chapter VII named as 'Offences and Penalties' (Clause 34-47). The aadhaar act offers an *"opportunity to a hearing"* to the Unique Identification Authority of India previous to the order of court related to the issue about the protection of data. Most importantly, an effort has been made to bring in a technical outline to control illegal surveillance by adding an Oversight Commission. It is supposed that this framework is diluted under Clause 33.

Under this Clause, there are two important aspects. Initially it is considered as an act to statement the difficulty of identification in a manner to deliver the social safety schemes to each and every individual. However, Clause 33 (2) says, "disclosure of information, including identity information or authentication records, made in the interest of national security," which proposes that the project of aadhaar project is not inadequate to enable the provision government supports and profits, but it can be utilizes for the purpose of surveillance and security.

In a way to defend obvious exploitation, this clause lays out "an Oversight Committee consisting of the

[35] PTI, Govt can not belittle Supreme Court order holding Aadhaar voluntary, Business Standard (May 05, 2017, 12:30 AM IST), http://www.business-standard.com/article/economy-policy/govt-cannot-belittle-supreme-court-order-holding-aadhaar-voluntary-117050401110_1.html.

[36] The Wire Analysis, As arguments on Aadhaar- Income Tax link end, the court may read down the mandatory provision, The Wire (May 05, 2017), https://thewire.in/132141/aadhaar-pan-supreme-court-income-tax/.

[37] Agencies, Linking Aadhaar to PAN contravenes Income Tax Act: Advocate Divan (Apr. 28, 2017), http://www.mid-day.com/articles/national-news-linking-aadhaar-to-pan-contravenes-income-tax-act-advocate-divan/18205169.

Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology." This committee would doing as a station to evaluate any illegal surveillance by the government.

Oversight Committee

Both the Indian Telegraph Rule 2007 and Indian Telegraph Act 1885 and had a 'Review Committee'. But, all of them had considerably unsuccessful to confine its mistreatment which is obvious from numerous cases from the previous two periods. According to year 2009, news derived out of Gujarat government's surveillance on a female architect; the 2010 Radia tapes disagreement exposed the nexus among politics, corporate and interception; in the year 2013 we caught of phone tapping which is unlawful by state agencies in the place related to Himachal Pradesh; in the year 2015 a commotion appeared among 2 currently separated states (Andhra Pradesh and Telangana) and scandal of phone-tapping raised apart from the several more claims by politicians regarding phone tapping. It specifies the deliberate misuse of surveillance by the state, which increases questions regarding the working of this planned misunderstanding committee.

Also, not like the United States' Foreign Intelligence Surveillance Court (1978) to control surveillance and United Kingdom's Investigatory Powers Tribunal (2008) and Intelligence and Security Committee of Parliament to supervise and observe illegal surveillance, India doesn't consider any such organised device. According to judgement report of Supreme Court of India in 1996 PUCL, it backed off from giving any previous legal scrutiny in matters of unlawful and data privacy surveillance. In its place, it specified that it is role of central government's to structure the laws and place the technical outline to control illegal surveillance. Hence, the formation of any institutional device occurred in hands of Parliament. But Clause 33(1) says "disclosure of information, including identity information or authentication records, [can be] made pursuant to an order of a court" this suggests that the parliament just set aside itself from taking the responsibility.

It is also mentioned in the paper as an example about, Goa court examined UIDAI to give the Central Bureau of Investigation the biometrics of everybody registered under Aadhar in the manner to support it resolve a case which is related to gang rape. In the year 2014, the Bombay High Court supressed and known incorrectly the judgement approved by the Goa High Court. This particular case reveals how in future times the judiciary can order the revelation of information related to biometric for CI or for cause of national safety.

With this power, the government will become like "big brother", watching our every activity plays on our worst fears. The worst thing is that if any aadhaar card holder wants to unregister oneself, it can't be done because there is no provision for this in the Aadhar Act.

Generally, this whole planned act reproduces the linking of expansion and surveillance mechanisms of state powers in the name of governance to place its citizens under surveillance. It is a central facilitation centre or technical interface, consisting an integrated requirement, which purposes to connect databases of around twenty-one categories (e.g. income tax, travel, and bank account details, driving licenses, telephone, immigration records and many more). In connection to that, it would be common with eleven central agencies (like IB, CBI, NIA, R&AW and many more.). It is, fundamentally, 'dataveillance' as it utilizes personal data systems in the examination and observing of the communications and actions of a person.

Interconnecting the card of biometric with that of the Intelligence Grid has authorised the Indian state having technologically-permitted surveillance. The massive record can be collectively with numerous other government departments and intelligence agencies. It also helps in a range of needs, containing those of domination, control, and safety. This increases the major danger of Aadhaar: its control as

a tool of mass surveillance. Including ready for all manner identification tool, the life of citizen will develop clear to the state as a contact lens. Particulars of phone call database, railway bookings, and financial connections and so on will be available to the government at the click of a mouse without invoking any extraordinary controls.

Lacunae in the aadhaar act

The aadhaar act before enactment was also debated in the Rajya Sabha. It proposed five changes in the Act, these changes were as follows-
CHANGE 1: Clause 3

A person who does not request to remain as of Aadhaar number card holder should be allowed to have his number removed from the Central Identities Data Repository. A certificate shall be allotted contained by request of around 15 days.

CHANGE 2: Clause 7

If an Aadhaar number is not allotted to or if a person's selects not to elect for registration, the individual shall be obtainable alternate and practical means of identification for supply of the benefits, subsidy, or service.

CHANGE 3: Clause 33

With the words "national security", the words "public emergency or in the notice of public safety" be relieved.

CHANGE 4: Clause 33

The Oversight Committee (which will take a conclusion on whether to decide to a request to share data of biometric of an individual for national safety) should also comprise the central vigilance commissioner or the 'comptroller and auditor general'.

CHANGE 5: Clause 57

Clause 57, which all prevent the state or anybody, company or person can use the Aadhaar number for creating the identity of an individual for any determination, should be deleted.

These changes seem to be very fair and reasonable however the bill was not amended again as it was presented as a money bill. But it can be said that the aadhaar act, before enactment has to be amended because following lacunae still existed in it.

No opt out option

The Aadhar Act doesn't deliver an opt-out clause, wherein Aadhar number holders can select enduringly detached from the Central Identities Data Repository.The aadhaar act indeed provides an opt-in option to the applicant.

No standard to take opt-in consent

According to section 8(2)(a) and (c) of the Aadhar Act require demanding entity to take the agreement of the individual previously gathering his/her identity information for the determinations of verification and also has to notify the individual of the changes to proposal of the identity information. Section 3(2) of the Act involve the registering actions to notify the individual about the way in which their information shall be shared and used confirm that their identity information is only require for proposal to the Central Identities Data Repository.

However, the Act deals with no standard or requirement for the procedure of agreement that must be engaged at the time of registration. This is important as it is the opinion at which persons are giving rare biometric material and throughout earlier registration, has been a point of weakness as the agreement was occupied is an enabler to purpose creep as it permits the UIDAI to distribute information with involved in the distribution of well-being facilities.

No limitation over collection of identity information

Section 3(1) of the Aadhar Act enables every "resident" to acquire an Aadhar number by give in to his/her biometric (fingerprint, photograph, Iris

scan) and demographic information (DOB, address, name).

It is also focused that the Act leaves opportunity for extra information to be comprised in the gathering process if so stated by regulations. It must be stated that though the Act precisely delivers what information can be gathered, it does not precisely forbid the gathering of additional information. This found to be important as it makes it possible for registering activities to gather additional information connecting to individuals in absence of any legal inferences of such activities.

The Act prohibits collection of the details about language, religion, tribe, caste, religion, race, caste, records of entitlement, ethnicity, income or medical record for the drive of Aadhaar verification but as evidenced by findings of an research organization Centre For Research in Internet and Society that this information is gathered by numerous agencies. Whereas this information should only be utilizes for the determination gathered, not only were the interior access controls among and around dissimilar agenecies of government agencies unobtainable on the portals, occurrences of caste information linked to Aadhaar being kept and found as reported for specific sites is also common together publicly on these portals.

No clarity whether the authorised personnel will Parliament for collecting the information which they are not authorised to collect

Section 36 of the Aadhaar Act stipulates that any individual who in not authorised to gather information under the Act, and imagines that he is authorised to do so, shall be illegal with custody for a term which may spread to 3 years or with a penalty which may spread to Rs. 10,000/- or both. In the situation of corporations, the extreme fine amount would be greater than before i.e. Rs. 1000000/-.

It must be well-known that the section, as it is presently expressed appears to criminalise the act of impression of official individuals and the real gathering of information is not mandatory to end this offence. It is also not specified if this section will put on person who is official to gather information under the Act in general, gathers some information that he/she is not official to assemble.

Access and correction

It is still not appropriate to access to the fundamental biometric information is not providing to an individual. Later, in Section 6 appears to place the accountability for informing and accurateness of biometric information on the individual, it is not identified that how an individual is theoretical to know that the biometric information controlled in the database has altered if he/she and does not have admittance to the same. The difficulty got more serious if we study that they can be incorrectly arrived in the system, as has been recognized in Rajasthan. It may also be well-known that the Aadhaar Act delivers only for an appeal (not demand) to the UIDAI for access to the information and does not create admittance to the information a right of the precise, this would mean that it would be completely at the pleasure of the UIDAI to decline to funding admission to the information when an appeal has been prepared.

Biometric information and Aadhaar numbers to be made public

It is uncertain for what determinations it would be essential for Aadhaar numbers and fundamental biometric information to be prepared public and it is regarding that such conditions are left to be well-defined by guideline. This is diverse from the Telegraph Act and the IT Act which describe the situations for an interruption in the Act and describe the process for carrying out interference orders in related Rules. Significant conditions for these information found to be public is beside the expose standards in the 43A Rules - which would be appropriate to the UIDAI and the expose of core biometric information.

Disclosure order related to Low standards

However a court order from a District Judge is required to authorise expose of information, the Act fails to describe significant values that related to

order must fulfil consisting that the order is essential and proportional. Revelations that are made ‘in the interest of national security' do not need approval by a judge and in its place can be sanctioned by the Joint Secretary of the Government of India - a standard less than recognized in the Telegraph Act and IT Act for the interruption of infrastructures.

Minimum rights for the citizen

Citizens Can’t Report Crimes Related to Aadhaar. A major concern is that the Aadhaar Act, 2016 strips legitimate citizens of their right to report criminal activities and breaches concerning Aadhaar.

Section 47 of the Aadhaar Act, 2016 effectively locks out any effective remedy for the affected person whose privacy has been impacted by the breach of Aadhaar numbers and other details. This Section provides that only on an objection made by UIDAI or any individual accredited by it, any Court can take awareness of any wrongdoing illegal under the Aadhaar Act, 2016. This effectively means that legitimate people, who are victims of breaches of their Aadhaar numbers or details, have no effective remedy.

Distressed workers considered choice of pending the consumer courts or continuing under Section 43A of the IT Act (for neglectful safety practices producing unfair loss or advance to a third party) previous an Adjudicating Officer, who can only perceive arguments less than Rs. 5 crores. Rule 5(9) of the 2011 IT Rules also envisions the selection of a Grievance Officer by corporates body. Though, in realism, such an officer is an 'invisible man', bearing in mind that the Rules are silent about his least qualifications, powers, tenancy, duration, and method of attaining a choice, and also no right of appeal is suggested.

Accountability

The operational management and compensation mechanisms needed for persons to be aware when there is an opening of privacy or expose of their private information. According to Section 47 of the Act suggests that only the UIDAI or its official officer can file an illegal complaint under the Act. Thus, all the illegal punishments recommended under the Act (like for revealing identity information under Section 37 or for unofficial access to the Central Identities Data Repository under Section 38) can only be introduced by the UIDAI, and not the distressed Aadhaar number holder.

There is no protest restored mechanism shaped under the Act. The power to set up these mechanism is given to the UIDAI under Section 23 (2) (s) of the Act. On the other hand, creating the entity managing a project , also liable for giving the outlines to address the grievances get up from the project, seriously concessions the freedom of the grievance redressal body. A self-determining national grievance redressal body with both district and state level bodies under it should be established.

Later, the NIAI Bill, 2010, providing for creating an Identity Review Committee to observe the practice pattern of Aadhar numbers. This has been detached in the Aadhar Act 2016 and must be reestablished.

Directness

There does not appear to be any facility in the Aadhaar Act which essential the UIDAI to formed its confidentiality procedure and policies present to the public in overall however the UIDAI has the duty to preserve the confidentiality and privacy of the information.

Undefined security measures

The act stipulates that suitable organizational and technical safety methods shall be put in place deprived of enlarging upon what those processes should be or describe any principles that they will follow to. The Act provide the Authority the influence to describe broad guidelines relating to security protocol.

Section 43 A Rules - Unclear application:

The act describes biometric facts composed as ‘sensitive personal data or information' under the Information Technology Act, 2000 and Section 43A Rules and statuses that Rules and Act would be

appropriate to information related to biometric. According to this case, than any corporate body (including the UIDAI) processing, gathering, or keeping biometric information would require to monitor the standards recognised in the Rules - comprising standards for consent, gathering, sharing, retention, disclosure and security. Yet, the Act permits the UIDAI to make rules for, expose, gathering, safety and many more.

Inefficient data protectin safeguards and unenforceable civil remedies

According to Section 30 of the Act, information related to biometric as "sensitive personal data or information", as understood in Section 43A of the Information Technology Act. Hence, IT act itself is not capable enough as far as the security of the private data is worried. The adjudicatory scheme for release of complex private data under the IT Act has physical faults and is not efficient. For example, Section 48 gives the establishment of multiple Cyber Appellate Tribunals, for applications in contradiction of the order of an Adjudicating Officer. Presently, Cyber Appellate Tribunal is the only which has been established in Delhi and even that has been non-operational since 2011. Hence, the last definite case appears to be of 30th June 2011, taking to bright the stark inadequacies of the operative of the IT Act. There is neither permanent seat nor court infrastructure for these cases and the refereeing officer who is generally the IT Secretary of the state government may not be qualified in legal point of view. Hence, the civil remedies obtainable in the Aadhaar Act looked to be unenforceable and illusionary.

No Criminal remedies for aggrieved person

Since under Section 47 of the Act only the UIDAI or its approved officer can file an illegal complaint under the Act, consequently, all the criminal punishments approved under the Act (e.g. for relating identity information under Section 37 or for unlawful access to the Central Identities Data Repository under Section 38) can only be originated by the UIDAI, and not the distressed holder of Aadhaar number.

Allows body commercial to utilize the aadhaar number for their own determination

The Aadhaar Act validates the storage, collection, and with the help of special data on the principle that it is a "condition for receipt of a subsidy, service or profit", as specified under Section 7 of the Act. Thus, the Act is described as regulating only the connections among the residents and its related State.

On the other hand, a deep appearance exposes that under Section 57, the Act also simplifies connections amomg the residents and private parties of India by permitting "body corporate" to utilize the Aadhar number for their own preference. This increases concerns about destructions of privacy when UIDAI distributes data continuing with private units.

In the cae, TrustID is known as an app that permits the operator to confirm any person with the help of their Aadhar number and deals with a range of services consisting credit background, pre-employment, tenants, employers, property vendors' and business partners validation. It is also not specified that the detail access by TrustID is compelling in means that look after individual's confidentiality.

These uses propose that the system of Aadhar will not be hardly incomplete to the submissions designated in the Section 7. The Act possibly shelters everybody. It can comprise all the connections directed by a person and the State in connection to subsidies and benefits; and the dealings among a separate and a corporate entity, where the confidential entity utilizes the Aadhar number for authentication and identification. The extended possibility of attention, connecting with the lack of defensive privacy, suggests that this Act has condensed complete privacy shields enjoyed by residents in India –hence in their connections with the State to contact subsidies/benefits or in their relations with commercial entities.

Notice

Method of providing notice left to the realm of regulations

Section 3(2) of the Aadhar Act needs that the works of registering individual for dispersal of Aadhar numbers should present individual notice concerning:

Method in which the information shall be utilizes;

Manner of receivers with the one information is planned to be distributed at the time of verification; and

Presence of right to access information, the process for creation desires for these required access, and specifics of the department or individual in responsibility to whom related requests can be made.

Section 8(3) of the Aadhaar Act needs that validating agencies shall provide details to the person's whose information is to be legitimate concerning

Manner of information that may be distributed upon verification;

Support to which the detailing established at the time of validation may be considered by the demanding entity; and

Substitutions to compliance of uniqueness detailing to the demanding entity.

At the same time it is well-known that the Act left the method of providing related announcement in the realm of rules and does not stipulate the reason behind the notice is to be provided, which miss significant essentials to the jurisdiction of executive. This left an uncertain picture as to how frequent, reachable, and comprehensive this sign essentially be.

No prescription of data breach notification

The Aadhar Act fails to recommend 'data breach notification' necessities, requiring the UIDAI to notify a person, the Aadhaar number holder, that their identity (demographic and biometric) information has been distributed or utilizes with absence of their consent as well as awareness.

Lack of an effective enforcement mechanism

According to Section 3(2) of the Act needed the joining agencies to notify the person about the way in which their related information utilizes and shared as well as confirm that their unique information is only important for submission to the Central Identities Data Repository.

Section 8(2) (b) and section (3) of the Aadhaar Act. The validating objects are permitted to utilize the self-information for the use of submission to the CIDR for validation. Later, Section 29(3) (a) of the Act stipulates that self-information presented to a demanding entity shall not be required for any manner except that definite to the person at period of authentication while defer to the information.

Also, Section 41 executes a punishment on the demanding entity for nonconformity.

Section 57 enables the state and the body corporates to use the aadhaar number holder's identity information. Section 37 of the Aadhaar Act provides that any verification entity which uses the information for any persistence not previously detailed will be responsible to a penalty of imprisonment of up to 3 years or a fine of Rs. 10,000/- or both. In point of view, companies, the extreme fine amount would be increased to Rs. 1000000/.

The absence of actual enforcement mechanism challenges these requirements. The Act does not detail how an Aadhaar number holder can intensify the issue (since only the UIDAI can file a complaint) or what standard will be utilizes to control whether the demanding entity has on condition that the information in a suitable and clear manner. There is no regulation governing the use of aadhaar number holder's information by third parties.

Section 33

Section 33 of the aadhaar act stipulates that the UIDAI may disclose identity information, verification records or any information in the CIDR subsequent a court order by a District Judge or more. Hence, order may only be formed after UIDAI is

permitted to perform in a hearing. According to section 33 of the Act, the confidentiality provisions in Sections 28 and 29 will not apply with esteem to revelation made in the interest of national security resulting instructions by a Joint Secretary to the Government of India, or an officer of a higher rank, official for this determination.

Disclosure provision in the act differs from the Indian Telegraph Act, 1885

The provisions adaptable expose of private information under the act diverge from guidelines stated under the Act differs from phone tapping guidelines in two ways. Initially, the act allowed sharing in the interest of 'national security' moderately for public safety or public emergency. Also, the order delivered by an officer of the rank of Joint Secretary, in its place of a home secretary.

Sweeping exception of National Security

According to Section 33(2), pares out an rapid exclusion to Section 29(1) (b)'s condition of "using" the information of biometric for any determination except the generation of numbers of Aadhaar and verification under this Act if it is in the attention of `national security'. The expression "national security" is indefinite in the Act, and also the General Clauses Act, and thus the situations in which a person's information may be revealed remnants open to understanding, consequently, section 33 is very imprecise.

No independent review of the order of disclosure of identity information under section 33(2)

According to Section 33(2), formed an exclusion to the confidentiality, security and disclosure provisions or requirements on the Joint Secretary direction in the notice of national security. These direction has to be go through by a 3 member of 'Oversight Committee', involving the Secretary of the Department of Legal Affairs, Cabinet Secretary, and the Secretary of the Department of Electronics and Information Technology. The secondary provision or condition later delivers that these direction considered to be lawful for about the duration of 3 months, later which it can be revised and prolonged further three months. This found to be difficult for numerous causes.

Meanwhile the overall review process of the revealing order is being maintained among the executive and there is no autonomous oversight.

Absence of defined responsibilities and functions of error mechanisms

According to Section 33 presently requires a process for misunderstanding by a committee, though, there are present no functional requirements placed as the controlling principles forming the powers and responsibilities of the mechanism which is oversight.

Lack of opportunity to data subject

The proviso in section 33(1) only involves a hearing to be specified to the UIDAI, and not to the one who is related to Aadhaar card holder, whose details is being revealed and in the sense of a court order information identification and records of authentication of person and can be exposed deprived of any opportunity or notice of hearing to the persons affected. The act does not offer any worth through which a person can challenge the order or contest it later it has been approved.

Involvement of private entity in the preservation and formation of the CIDR

Section 10 of the Act stipulates that the Authority may involve one or more things to create and preserve the Central Identities Data Repository and to accomplish any other related meanings as may be detailed through principles and rules.

In case of private object is considered in the establishment and maintenance of CIDR and can be supposed that there is the chances that they would, to some extent, have admittance to the information kept in the CIDR, yet there are no perfect standards in the Act concerning this possible admittance and the development for engaging related entities. The fact that the UIDAI has been specified the independence to engage an exterior object to preserve a delicate

asset like CIDR increases the apprehensions related to safety.

Interest Conflict

The Courts cannot consider awareness of any felony illegal under the Act except an objection is prepared by the expert of UID or an individual sanctioned by it. It is distinct UID will criticise in contradiction of the aforementioned in the case related to breach.

Failure of the aadhaar

According to official data consider on the website of Telangana government, the verification rate of failure on the basis of Aadhar transactions was around 36% for the period among January to the present date; this was more than the rate of failure of upto 34% recorded in the dated of October-December earlier year. Also, the rate of failure in the two districts of Wanarapathy and Adilabad were as more than in the time duration of 1 January and 6 April around 38% 46% respectively. The Aadhar biometric verification rate of failure in the determined job of rural guarantee structure is as more as approximately 36% in Telangana, data organized by the state government observe. The chief cause for the failure of payment in the procedure of the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) was the biometric disparity, as per as the data represent. Because of the wear and tear of their fingers, the rural labourers have unsuccessful the verification of biometric. Hence, iris scanners, mostly with the reason that they are costly, have not been organized broadly, the related workers have been deprived of income payments because of them. This rate of failure is certainly very troublesome as it is disturbing the living condition of an individual. The case related to ATMs, delivers the rate of failure is only around 0.5%. And for the purpose of Aadhar verification for MGNREGA social safety pensions and pays, the failure rate is as maximum as 30%. 22% of PDS holders of card in Andhra Pradesh could not gather their rations shares due to failure of fingerprint authentication in approximately 290 of the 790 cardholders, and in 93 occurrences there was an ID disparity as well. A current paper by Hans Mathews (mathematician with the CIS) on the Economic and Political Weekly, represent the program would fail to exceptionally recognize the individuals in a nation of about 1.2 billion. This importance represent that difficulty is with the technology of Aadhar particularly when it is related to biometric disparities.

Conclusion

In today's world smartphones, CCTV camera, drones, social media and many such technologies are producing sensitive and personal data which definitely have the capability of threatening the privacy of the people and thereby risking their financial and personal security. Aadhaar, a go-to document to access numerous public services, is another tool to harness biometric and demographic data in large volumes. There is a legitimate fear that this identity technology will open us all up to discrimination, prejudice, the risk of identity theft and subject the entire population of the country under continuous surveillance. However even if existing legal frameworks on Aadhaar are sketchy and not adequate, aadhaar can't be abandoned merely for these suspected risk. Aadhaar Identity information under aadhaar is very well protected in the CIDR. Not a single instance of data-breach from CIDR has been noticed. There are some instances of disclosure of aadhaar number and personal information by some government departments but the absence of any legal provision to deter these disclosures is to be blame for this, not aadhaar and its technology. It is only sporadic and episodic, it only verifies the identity of the person during authentication which is not surveillance. It will mean to be surveillance when UIDAI the purpose for which the aadhaar is being used and when the UIDAI is black-boxing information.

The aadhaar act lacks Security of the personal identity information, openness in the working of the UIDAI, proper supervision, redress mechanisms and accountability of the oversight committee. It only requires specific amendments to insert some

procedural safeguard measures for the security of the data and the privacy of the citizens to remove all these lacunae. Other than these the technology also needed to be improved to protect data from cyber terrorism which can't be done instantly. Technology isn't foolproof and there is no method to make it entirely safe. In this complex and evolving technology errors are inevitable. For instance, across its products, Google has to achieve around 2 billion lines of basis code. The average program has 14 distinct susceptibilities, each of them a possible of illicit entrance. Such flaws are compounded by the history of the Internet, in which security was a late addition. But this is not to suggest not to do anything for data protection for technology is so complex. Instead, there is an urgent need to generate a larger conversation involving all the private stakeholders to remove all the misconception about right to privacy.

The right to Privacy is not considered an absolute right but a right having layers of importance depending upon the substance that is deemed to be kept private and opposite interest, for example, national security or investigation of a crime, for which privacy can or can't be compromised. Research. If the substance is biometric or personal information but the opposite interest is very compelling like national security then the importance of the right to privacy would not be more than national security. If the nation gets rid of terror financing, corruption, duplicated passport, sim, driving licence and evasion of tax etc. by making aadhaar mandatory then it has to be done. However, an existing delicate balance between these opposite interests should be maintained by an accountable and transparent oversight committee to ensure that Aadhaar should not become a tool for misuse of people's information. Numerous checks and balances need to be put in place for ensuring the security and stability of the Aadhaar ecosystem. This is not just significant from the viewpoint of individuals, even companies and countries are vulnerable (hackers mostly go after institutions, which curate all kinds of information).

Aadhaar technology if used wisely can transform the nation. If not, it can cause us untold harm. We need to be prepared for the impending flood of data—we need to build dams, sluice gates and canals in its path so that we can guide its flow to our benefit. It is high time that the biggest democracy of the world takes cognisance of the intrinsic legal, policy and regulatory deficiencies in the Aadhaar ecosystem

.