Xournals

Academic Journal of Law and Judiciary

ISSN: UA | Volume 01 | Issue 01 | April-2018

Aadhaar- The Basis of an Indian

Yogesh Chalisa[1]

Available online at: www.xournals.com

Received 12th January 2018 | Revised 1st February 2018 | Accepted 13th April 2018

Abstract:

Since its inception in 2009, the Aadhaar project has been shrouded in controversy due to various questions raised about privacy, technological issues, welfare exclusion, 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 Tanzania, Afghanistan, Bangladesh, Russia, Morocco, Algeria, and Tunisia, have expressed interest in the system . Government asserted Supreme Court, by linking Aadhar to PAN card will weed out fake PAN cards which are used for terror financing, drug financing, and circulation 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. *National Law Institute University Bhopal, 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 (photograph, fingerprint, iris scan etc.) and personal information (name, date of birth, address etc) of the people. National Identification Authority of India Bill, 2010 (hereinafter as the NIAI Bill) was introduced 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 enactment of legislation of a data protection and privacy is was a pre-requisite for the Aadhaar scheme." But the project was continued to be executed without any legislation. A new bill, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 (hereinafter Aadhaar Act, 2016) finally get enacted. 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 maintenance and establishment 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 Supreme Court's interim order dated August 11 and October 15, 2015, made an amendment and inserted Section 139AA in the Income Tax Act, which made aadhaar mandatory for the filing of income tax returns 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 Tanzania, Afghanistan, Bangladesh, Russia, Morocco, Algeria, and Tunisia, have expressed interest in the system[3].Government, reportedly, per year saves approximately USD 1 billion (Rs 650 crores) transfer cost under Mahatma Gandhi National Rural Employment Guarantee Act, supplying of LPG subsidy, disbursement of pension, provident fund and ration under PDS scheme. The government asserted Supreme Court, by linking Aadhaar to PAN card will weed out fake PAN cards which are used for terror financing, drug financing, and circulation 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 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

[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.

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 Tanzania, Afghanistan, Bangladesh, Russia, Morocco, Algeria, and Tunisia, have expressed interest 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 to PAN card will weed out fake PAN cards which are used for terror financing, drug financing, and circulation 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

The decision to use the 12 digits individual identification number on Aadhar card for Direct Benefit Transfer (DBT) for individual beneficiaries under social welfare schemes was made to stop duplicate applicants, frauds, and middleman and end corruption within government. It is now being used to get LPG subsidy, availing of other subsidies without the need to register and enrol for these separately, monthly pension, provident fund and scholarships for the students directly in the bank account. This negates the possibility of the funds being misappropriated or of individuals making fraudulent claims in order to claim benefits. A cumulative amount of Rs 17869475 has been transferred using DBT for 138 schemes under 27 ministries since 2013. 29 various financial frameworks like Aadhaar Payments Bridge (hereinafter referred as APB) and Aadhaar Enabled Payment Systems (hereinafter referred as AePS) have been built by National Payment Corporation of India to support DBT and also to allow individuals use Aadhaar for payments. In the PDS scheme alone almost Rs 14,000 crore has been saved.[8]

Universal Identification-

The Aadhaar card is a universal card that does not really have a specific purpose behind it. Unlike a voter ID card, whose sole purpose is to permit the holder to take part in the electoral process, the Aadhaar card the with any specific use in mind. Instead, it can be used for a number of purposes, making it a universally acceptable government-issued card, without needing to register or apply for a separate card for each of these services. For example, an Aadhaar card can be used as proof of identity, proof of address as well as proof of age when applying for any government service.

Ease of Availability:

The Aadhaar card is the only government-issued document that is available anywhere, everywhere. An Aadhaar card can be applied for online. Known as e-Aadhar, this is the downloadable version of your Aadhaar card and can be accessed wherever and whenever required. This makes it convenient for individuals to always have a copy of a valid government-issued identity document that is also easily accessible. This also reduces the risk of a document being stolen/misplaced, since the Aadhaar can be downloaded onto any device and displayed when required.

[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

Digital Life Certificate

The 'Jeevan Praman for Pensioners' or the Digital Life Certificate as it is also called, was initiated by Department of Electronics and IT with the aim of abolishing the need for the pensioner to be physically present in order to receive the pension for the continuation of their scheme. Pensioners can now avail pension without having to leave their homes as their details can be digitally accessed by the agency through their Aadhaar Card numbers.

Digital Locker:

The government of India has launched digital locker (DigiLocker) system for everyone for storing all personal documents on the government's server. The sign-up process for DigiLocker requires a person to link his/her 12 digit Aadhaar card number.

Voter Card Linking:

Starting 9th March 2015, Aadhaar card UIDAI number would be linked to the voter ids. This action is taken to eliminate bogus voters. Once an Aadhaar number is linked, it would become impossible for a multiple voter ID card holder to make its illegal use, as registration requires voter card holder to be physically present and produce Aadhaar card to the polling booth officer for linking.

Removed bottlenecks from the bureaucracy

By using Aadhaar Card, passports can now be availed by applicants within 10 days. Individuals who wish to obtain a passport can apply for the same online by simply attaching their Aadhaar Card as the only residence and identity proof along with their application. Financial institutions and banks consider Aadhaar Cards as a valid address and photo ID proofs during the time of opening a bank account. It is used for KYC, identification and verification purposes. Banks are issuing basic banking or "no-frills account" under Jan Dhan Yojna using Aadhaar as the primary authentication for individuals to receive benefits from government schemes.[9] For the migrant population in cities, who live in slums or unauthorised clusters and keep shifting homes, any work that required them to provide proof of identity and residence – opening a bank account, applying for a ration card or even a gas connection – was always a problem. Aadhaar gave them an identity document that would remain valid wherever they moved.

Controversies surrounding the Aadhaar and their analysis

Since its inception in 2009, the Aadhaar project has been shrouded in controversy due to various questions raised about privacy, technological issues, welfare exclusion, and security concerns.[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 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 parliamentary standing committee, led by 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 (Targeted Delivery of Financial and other Subsidies, benefits and services) Act (hereinafter as the aadhaar Act) was enacted 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 "requesting entity" (any "agency or person" who is willing to pay the fees) can ask for any aspect of that person's identity information including photograph, except for the core biometric information to be shared during authentication provided the requesting entity must inform the Aadhaar card holder about the use it proposes to make of identity information 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

[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

accessible. For instance, before buying sim card using aadhaar, it would be unpractical to expect from any person to read the fine print of the terms and conditions, or before clicking "I agree" when installing new software. And after taking nominal consent by this way there is nothing that can prevent a requesting entity from sharing the identity information (name, address, date of birth, photograph – whatever the government decides).[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 to be done by registrars which are mainly government and public sector agencies. But they can hire enrolment agencies which can be private players, to collect demographic and biometric information and these enrolment agencies can hire enrollment operators and supervisors through third parties. The aadhaar act lacks any provision for a foolproof system in place to guard against the breach of data from any of these points or to ensure that enrolment agencies and operators do not keep a copy of the database when they hand it over to the government. There are some instances reported when enrolment agencies and operators handle the information, available to them, in a casual manner.[12]

Disclosure of the aadhaar numbers

Various agencies in the country collect different information for statistical purpose empowered by the Collection of Statistics Act, 2008.[13] This information is collected by publishing a notification in the official Gazette and Section 9(4) prohibits the publication of identifying information unless permitted by the concerned person. Similarly, the publication of Aadhaar numbers is also prohibited under Section 29 (4) of the Aadhaar Act, 2016 unless the permission to publish them is sought from the Aadhaar number holder. 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 Centre for Internet and Society in Bangalore reported that an estimated 135 million Aadhaar numbers had been leaked online from four separate government databases.[14] The first two belong to the rural development ministry—the National Social Assistance Programme (NSAP)'s dashboard and the National Rural Employment Guarantee Act's (NREGA) portal. The other two databases deal with Andhra Pradesh—the state's own NREGA portal and the online dashboard of a government scheme called "Chandranna Bima". The type of data disclosed included names, names of parents, PAN numbers, mobile numbers, religions, marks, the status of Aadhaar applications, 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 personally identifiable information of beneficiaries or subjects of the databases containing Aadhaar numbers of individuals along with other personal identifiers. All of these disclosures are symptomatic of a significant and potentially irreversible privacy harm.[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

[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

[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.

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 dashboard of a government scheme called "Chandranna Bima" may be laudable for providing easy access to government data condensed for easy digestion, however in the absence of proper controls exercised by the government departments populating the databases which inform the data on the dashboards, the results can be disastrous by divulging sensitive and adversely actionable information about the individuals who are responding units of such databases.[19] Through aadhaar number and some basic identity information, other granular details about individuals including sensitive PII such as caste, religion, address, photographs and details of bank account details, credit card numbers and passwords can easily be accessed through social engineering to steal money from individual's accounts.[20] One of the prime examples is individuals receiving phone calls from someone claiming to be from the bank.[21] Another method is changing the phone number linked to aadhaar number maliciously. There are also some brokers which buy tonnes of copies of Aadhaar documents from shops selling SIM cards and other institutions, for the purposes of identity fraud.[22] In the recent past, there have been reported cases of employees of services provider caught stealing the biometric data collected for Aadhaar authentication.[23] It has been stated by the government that so far 34000 operators have been blacklisted for enabling the creation of fake Aadhaar numbers.[24] Even biometric data can be collected, for example lifting people's fingerprints remotely and without consent from a variety of objects that they may touch, and their iris data may be picked up by a high resolution, directional camera from a distance.[25] In light of these factors, the public presence of Aadhaar numbers, details about DBT transfers, registered mobile phone numbers and seeded bank account numbers presents a huge opportunity for financial fraud. In the US, the ease of getting Social Security Numbers from public databases has resulted in numerous cases of identity theft.[26] These risks increase multifold in India due to the mapping of the aadhaar number with bank accounts under Aadhaar Payments Bridge (APB) and Aadhaar enabled Payment Systems (AePS).[27]

In case a financial fraud takes place through AePS, the consumer may not be able to assert his claims for compensation due to the terms and conditions around liabilities, these terms force the consumer to take liabilities onto oneself than the payment provider. The terms and conditions have been vague in the recent AePS applications like BHIM Aadhaar App.[28] Regulations and standards around Aadhaar are at a very early and nascent stage causing an increase in

[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.

[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.

financial risk for both consumers and banks to venture into AePS.[29]

Over delegation of powers to the UIDAI

The matters on which the UIDAI may frame rules include:

The process of collecting information, Verification of information, Individual access to information, Sharing and disclosure of information, Alteration of information, Request and response for authentication, Defining use of Aadhaar numbers, Defining privacy and security processes, Specifying processes relating to data management, security protocols and other technology safeguards under this Act and Establishing grievance redressal mechanisms.

This Act allows the executive a very high degree of discretionary power. As mentioned above, a number of important powers which should ideally be within the purview of the legislature are delegated to the UIDAI. The UIDAI has been administrating the project since its inception, and a number of problems have already been documented in the process such as collection, verification, sharing of information, privacy and security processes. Rather than addressing these problems, the Act allows the UIDAI to continue to have similar powers. Even the power to set up such a mechanism is delegated to the UIDAI under Section 23 (2) (s) of the Act despite the fact that making the entity administering a project, also responsible for providing for the frameworks to address the grievances arising from the project, severely compromises the independence of the grievance redressal body.

No Effective Provisions for Cybersecurity

The biometric and demographic information of persons collected under the Act is stored in a centralised database called 'Central Identities Data Repository' (CIDR), which is under the control of Unique Identification Authority of India (UIDAI).

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter 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 security of identity information and authentication records of individuals stored 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]

[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

[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.

Taking cognizance of bodily interest and personal interest of individuals Supreme Court held on August 11 and October 15, 2015, in unambiguous terms, that Aadhaar could not be made mandatory, and that it could be used only for the six purposes specified by the government before 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 despite the Supreme Court ruling that this should not be done. Seeking consent for linking the Aadhaar number with the bank account means nothing when banks insist on customers providing Aadhaar numbers. Income tax assessees are being asked to provide their aadhaar numvers from assessment year. The Election Commission is putting out advertisements asking people to link their Aadhaar numbers with their election identity cards. 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 parliament also made an amendment and inserted Section 139AA of the Income Tax Act which provides for mandatory quoting of Aadhar or enrolment ID of Aadhar application form for filing of income tax returns and making application for allotment of PAN number with effect 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. Judgment or order of the Supreme Court is not cast in stone and as many as 30 judgments of the Supreme Court have been reversed by parliament, but in all previous cases, parliament took care to change the basis of a judgment before overruling it. In this case also if the government wants to make aadhaar mandatory then it should amend the Aadhaar Act to make it mandatory 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 making Aadhaar mandatory for filing 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 confusion over whether it is voluntary or mandatory and whether the lack of it can be used to deny someone a service. Related to this is the fact that it will become a single point of access to information about everything concerning an individual, which is why the privacy issue is paramount.

Surveillance

Under the aadhaar Act, the most controversial subject of security and privacy of individuals' electronic data is dealt with in Chapter VI of Protection of Information. In Clause 30, biometric and demographic information is regarded as *"electronic record,"* and *"sensitive personal data or information"* as mentioned in the Information Technology Act, 2000. If any individual or company impersonates, intentionally discloses, transmits, copies or disseminates, damages, steals, conceals, destroys, deletes or alters, or tampers with etc. such vital information, it is to be regarded as an offence which is elaborated in Chapter VII titled 'Offences and Penalties' (Clause 34-47). The aadhaar act gives an *"opportunity to a hearing"* to the Unique Identification Authority of India prior to the court's order relating to any matter of protection of information. Most importantly, an attempt has been made to bring in a procedural framework to curb

[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/.

[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.

unlawful surveillance by adding an Oversight Committee. It is alleged that this framework is diluted under Clause 33.

Under this Clause, there are two significant aspects. Firstly, it is regarded as an act to address the problem of identification in order to provide social security schemes to every individual. However, Clause 33 (2) says, *"disclosure of information, including identity information or authentication records, made in the interest of national security,"* which suggests that the aadhaar project is not limited to facilitate delivery government subsidies and benefits, but it can be used for security and surveillance.

In order to protect blatant misuse, this clause lays out *"an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology."* This committee would act as a channel to review any unlawful surveillance by the government.

Oversight Committee

Indian Telegraph Act 1885[38] and Indian Telegraph Rule 2007[39] and both of them had a 'Review Committee'. But, all of them had substantially failed to restrain its misuse which is evident from several cases from the last two decades. In the 2009 news came out of Gujarat government's surveillance on a woman architect; the 2010 Radia tapes controversy revealed the nexus between corporate, politics and interception; in 2013 we heard of illegal phone tapping by state agencies in Himachal Pradesh; in 2015 a clash emerged between two recently bifurcated states (Telangana and Andhra Pradesh) and phone-tapping scandal surfaced apart from the many more allegations of phone tapping by the politicians. It indicates the blatant misuse of surveillance by the state, which raises questions about the functioning of this proposed oversight committee.

Secondly, unlike the United States' Foreign Intelligence Surveillance Court (1978) to regulate surveillance and United Kingdom's Investigatory Powers Tribunal (2008) and Intelligence and Security Committee of Parliament to oversee and examine unlawful surveillance, India does not have any such institutional apparatus. The Supreme Court of India in 1996 PUCL judgement clearly backed off from providing any prior judicial scrutiny in matters of data privacy and unlawful surveillance. Instead, it stated that it is the central government's role to frame laws and lay down the procedural framework to curb unlawful surveillance. Hence, the creation of any institutional apparatus lies 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*.

A Goa court asked UIDAI to give the Central Bureau of Investigation the biometrics of everyone enrolled under Aadhar in the state to help it solve a gang rape case.[40] In 2014, the Bombay High Court quashed and called erroneously the judgement passed by the Goa High Court. This case reflects how in coming times the judiciary can order the disclosure of biometric information for criminal investigation or for reasons of national security.

With this power, the government will become like "big brother", watching our every activity plays on our worst fears.[41] 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.[42]

Overall, this entire proposed act reflects the interlocking of surveillance mechanisms and expansion of state powers to put its citizens under surveillance in the name of governance. Post 26/11 Mumbai attack, India's intelligence gathering and action networks were retreaded by launching NATGRID (National Intelligence Grid). It is a technical interface or central facilitation centre, with an integrated facility, which aims to link databases of 21 categories (e.g. travel, income tax, driving licenses, bank account details, immigration records, telephone etc). In addition to that, it would be shared with 11 central agencies (eg. CBI, IB, R&AW, NIA etc.). It is,

[38] Indian Telegraph Act, 1885, Section 5.
[39] Indian Telegraph Rule, 2007,Section 419A.
[40] The Indian Express, Stop Aadhaar data use to probe crime: UIDAI to SC, The Indian Express (Mar. 19, 2014, 12:50 IST), http://indianexpress.com/article/india/india-others/stop-aadhaar-data-use-to-probe-crime-uidai-to-sc/.
[41] Anil Padmanabhan, Aadhaar: in the eye of the privacy storm, Live Mint (Apr. 10, 2017, 03: 50 AM IST), http://www.livemint.com/Opinion/AF15Svbru1pCvHwV8AYDPP/Aadhaar-In-the-eye-of-the-privacy-storm.html?li_source=LI&li_medium=news_rec.
[42] Jean Dreze, Hello aadhaar goodbye privacy (Mar. 24, 2017), https://thewire.in/118655/hello-aadhaar-goodbye-privacy/

essentially, 'dataveillance' as it uses personal data systems in the investigation and monitoring of the actions or communications of an individual.

Interlocking the biometric card with the Intelligence Grid has empowered the Indian state with technologically-enabled surveillance. The colossal database can be shared with various other intelligence agencies and government departments. It also serves a range of desires, including those of control, governance and security. This raises the biggest danger of Aadhaar: its power as a tool of mass surveillance. By such an all-purpose identification tool, the life of citizen will become transparent to the state as a contact lens. Courts can order UIDAI to provide law enforcement agencies with the biometrics for an entire state (as the Bombay high court did) to check if they match against the fingerprints recovered from a crime scene. Details of railway bookings, phone call records, and financial transactions and so on will be accessible to the government at the click of a mouse without invoking any special powers.

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

An individual who does not wish to continue as a holder of Aadhaar number should be permitted to have his number deleted from the Central Identities Data Repository. A certificate shall be issued within fifteen days of the request.

CHANGE 2: Clause 7

If an Aadhaar number is not assigned to or if an individual chooses not to opt for enrollment, the person shall be offered alternate and viable means of identification for delivery of the subsidy, benefits, or service.

CHANGE 3: Clause 33

For the words "national security", the words "public emergency or in the interest of public safety" be substituted.

CHANGE 4: Clause 33

The Oversight Committee (which will take a decision on whether to agree to a request to share biometric data of an individual for national security) should also include 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 establishing the identity of an individual for any purpose, should be deleted.[43]

These changes seem to be very fair and reasonable however the bill was not amended again as it was introduced 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 does not provide an opt-out clause, wherein Aadhar number holders can choose permanently removed 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 requesting entity to take the consent of the individual before collecting his/her identity information for the purposes of authentication and also has to inform the individual of the alternatives to submission of the identity information. Section 3(2) of the Act require the enrolling agencies to inform the individual about the manner in which their information shall be used and shared and ensure that their identity information is only used for submission to the Central Identities Data Repository.

However, the Act provides no requirement or standard for the form of consent that must be taken during enrollment. This is significant as it is the point at which individuals are providing raw biometric material and during previous enrollment, has been a point of weakness as the consent was taken is an enabler to function creep as it allows the UIDAI to share information with engaged in the delivery of welfare services.

[43] 5 changes Rajya Sabha wanted in Aadhaar Bill, Rediff Business (Mar. 17, 2016, 02:06 PM IST), http://www.rediff.com/business/report/changes-rajya-sabha-wanted-in-aadhaar-bill/20160317.htm.

No limitation over collection of identity information

Section 3(1) of the Aadhar Act entitles every "resident"[44] to obtain an Aadhar number by submitting his/her biometric (photograph, fingerprint, Iris scan) and demographic information (name, date of birth, address).

It must be noted that the Act leaves scope for further information to be included in the collection process if so specified by regulations. It must be noted that although the Act specifically provides what information can be collected, it does not specifically prohibit the collection of further information. This becomes relevant because it makes it possible for enrolling agencies to collect extra information relating to individuals without any legal implications of such actions.

The Act prohibits collection of the details about religion, caste, race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history for the purpose of Aadhaar authentication but as evidenced by findings of an research organization Centre For Research in Internet and Society that this information is collected by various agencies. While this information should only be used for the purpose collected, not only were the internal access controls within and across different government agencies unavailable on the portals, instances of caste information linked to Aadhaar being stored and found as reported for specific sites is also shared both publicly on these portals.[45]

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 person who in not authorised to collect information under the Act, and pretends that he is authorised to do so, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to Rs. 10,000/- or both. In the case of companies, the maximum fine amount would be increased to Rs. 1000000/-.

It must be noted that the section, as it is currently worded seems to criminalise the act of impersonation of authorised individuals and the actual collection of information is not required to complete this offence. It is not clear if this section will apply if a person who is authorised to collect information under the Act in general, collects some information that he/she is not authorised to collect.

Access and correction

It is not clear why access to the core biometric information is not provided to an individual. Further, since Section 6 seems to place the responsibility for updating and accuracy of biometric information on the individual, it is not clear how a person is supposed to know that the biometric information contained in the database has changed if he/she does not have access to the same. The problem gets more severe if we consider that they can be wrongly entered in the system, as has been documented in Rajasthan[46] (where the biometric information of potential food ration beneficiaries did not match the data stored on the Aadhaar servers). It may also be noted that the Aadhaar Act provides only for a request (not demand) to the UIDAI for access to the information and does not make access to the information a right of the individual, this would mean that it would be entirely at the discretion of the UIDAI to refuse to grant access to the information once a request has been made.

Aadhaar numbers and biometric information to be made public

It is unclear for what purposes it would be necessary for Aadhaar numbers and core biometric information to be made public and it is concerning that such circumstances are left to be defined by regulation. This is different from the Telegraph Act and the IT Act

[44] Section 6 of the Income Tax Act says defines A resident is defined as any person who has resided in India for a period of at least 182 days in the previous 12 months.

[45] 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

[46] Anumeha Yadav, Rajasthan presses on with Aadhaar after fingerprints readers fail: We'll buy iris scanners (Apr. 10, 2016, 09:00 AM IST), https://scroll.in/article/806243/rajasthan-presses-on-with-aadhaar-after-fingerprint-readers-fail-well-buy-iris-scanners.

which define the circumstances for an interception in the Act and define the procedure for carrying out interception orders in associated Rules. Defining circumstances for such information to be made public is against the disclosure standards in the 43A Rules - which would be applicable to the UIDAI and the disclosure of core biometric information.

Low standards for disclosure order

Though a court order from a District Judge is required to authorise disclosure of information, the Act fails to define important standards that such an order must meet including that the order is necessary and proportionate. Disclosures that are made 'in the interest of national security' do not require authorization by a judge and instead can be authorised by the Joint Secretary of the Government of India - a standard lower than that established in the Telegraph Act and IT Act for the interception of communications.

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 a complaint made by the UIDAI or any person authorised by it, any Court can take cognizance of any offence punishable 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.

Aggrieved users only have the option of approaching the consumer courts or proceeding under Section 43A of the IT Act (for negligent security practices causing wrongful loss or gain to a third party) before an Adjudicating Officer, who can only hear disputes less than Rs. 5 crores. Rule 5(9) of the 2011 IT Rules also envisages the appointment of a Grievance Officer by body corporates. However, in reality, such an officer is an 'invisible man', considering that the Rules are silent about his minimum qualifications, duration, tenure, powers, and manner of reaching a decision, and no right of appeal is prescribed.[47]

Accountability

Effective supervision and redress mechanisms require individuals to be informed when there is a breach of confidentiality or disclosure of their personal information. Section 47 of the Act prescribes that only the UIDAI or its authorised officer can file a criminal complaint under the Act. Thus, all the criminal penalties prescribed under the Act (e.g. for disclosing identity information under Section 37 or for unauthorised access to the Central Identities Data Repository under Section 38) can only be initiated by the UIDAI, and not the aggrieved Aadhaar number holder.

There is no grievance redressal mechanism created under the Act. The power to set up such a mechanism is delegated to the UIDAI under Section 23 (2) (s) of the Act. However, making the entity administering a project[48], also responsible for providing for the frameworks to address the grievances arising from the project, severely compromises the independence of the grievance redressal body. An independent national grievance redressal body with state and district level bodies under it should be set up. Further, the NIAI Bill, 2010, provided for establishing an Identity Review Committee to monitor the usage pattern of Aadhar numbers. This has been removed in the Aadhar Act 2016 and must be restored.[49]

Openness

There does not seem to be any provision in the Aadhaar Act which requires the UIDAI to make its privacy policies and procedure available to the public in general even though the UIDAI has the

[47] Vrinda Bhandari and Renuka Sane, Analysing the Information Technology Act (2000) from the viewpoint of protection of privacy (Mar. 18, 2016), https://ajayshahblog.blogspot.nl/2016/03/analysing-information-technology-act.html.

[48] Section 23(2) (s) of the Aadhaar Act.

[49] Amber Sinha, Sandro Chattapadhayay, Sunil Abraham and Vanya Rakesh, List of Recommendation on the Aadhaar Bill, 2016- Letter Submitted to the Members of Parliament (Mar. 16, 2016), http://cis-india.org/internet-governance/blog/list-of-recommendations-on-the-aadhaar-bill-2016.

responsibility to maintain the security and confidentiality of the information.

Undefined security measures

The act specifies that appropriate technical and organisational security measures shall be put in place without elaborating upon what those measures should be or define any standards that they will adhere to. The Act gives the Authority the power to define broad regulations pertaining to security protocol.

Unclear application of Section 43 A Rules:

The act characterises biometric information collected as 'sensitive personal data or information' under the Information Technology Act, 2000 and Section 43A Rules and states that the Act and Rules would be applicable to biometric information. If this is the case, than any corporate body (including the UIDAI) collecting, processing, or storing biometric information would need to follow the standards established in the Rules - including standards for collection, consent, disclosure, sharing, retention, and security. Yet, the Act allows the UIDAI to make regulations for collection, disclosure, security etc.

Inefficient data protection safeguards and unenforceable civil remedies

Section 30 of the Act treats biometric information as "sensitive personal data or information", as understood in Section 43A of the Information Technology Act. But the IT act itself is not efficient enough as far as the protection of the private data is concerned. The adjudicatory system for disclosure of sensitive personal data under the IT Act has structural flaws and is not functional[50]. For instance, Section 48[51] provides for the establishment of multiple Cyber Appellate Tribunals, for appeals against the order of an Adjudicating Officer. Currently, only one Cyber Appellate Tribunal has been set up in Delhi and even that has been defunct since 2011[52]. In fact, the last decided case seems to be of 30th June 2011[53], bringing to light the stark inefficiencies of the functioning of the IT Act. There is neither court infrastructure nor permanent seat for such cases and the adjudicating officer who is usually the IT Secretary of the state government may not be trained in law. Hence, the civil remedies offered in the Aadhaar Act appeared to be illusionary and unenforceable.[54]

No Criminal remedies for aggrieved person

Since under Section 47 of the Act *only* the UIDAI or its authorised officer can file a criminal complaint under the Act, therefore, all the criminal penalties prescribed under the Act (e.g. for disclosing identity information under Section 37 or for unauthorised access to the Central Identities Data Repository under Section 38) can only be initiated by the UIDAI, and not the aggrieved Aadhaar number holder.

Allows body corporate to use the aadhaar number for their own purpose

The Aadhaar Act justifies the collection, storage, and use of personal data on the premise that it is a "condition for receipt of a subsidy, benefit or service", as stipulated under Section 7 of the Act. Thus, the Act is portrayed as covering (or regulating) only the interactions between the State and its residents.

However, a closer look reveals that under Section 57, the Act also facilitates interactions between private parties and residents of India by allowing "body corporate" to use the Aadhar number for their own purpose. This raises concerns about violations of privacy when UIDAI shares data with private entities.

For instance, TrustID is an app that allows the user to verify any individual using their Aadhar number and offers a range of services including pre-employment, credit background, tenants, business partners, employers, and property owners' verification. It is not clear that the information access by TrustID is taking place in ways that protect the privacy of individuals.

[50] Anumeha Yadav, The government has introduced a bill on Aadhaar and it is not good news (Mar. 05, 2016, 10:30 AM IST), https://scroll.in/article/804577/the-government-has-introduced-a-bill-on-aadhaar-and-it-is-not-good-news.

[51] Available at https://indiankanoon.org/doc/1414109/.

[52] Soibam Rocky Singh, India's only cyber appellate tribunal defunct since 2011, Hindustan Times (Jun 29, 2017, 11:37 IST), http://www.hindusta%3Ctimes.com/india/india-s-only-cyber-appellate-tribunal-defunct-since-2011/story-208HGrEN7hXrABg7lAb69N.html.

[53] http://catindia.gov.in/judgement.aspx

[54] Anumeha Yadav, Seven reasons why Parliament should debate the Aadhaar bill (and not pass in a rush (Mar. 11, 2016, 09:15 AM), https://scroll.in/article/804922/seven-reasons-why-parliament-should-debate-the-aadhaar-bill-and-not-pass-it-in-a-rush.

These applications suggest that the Aadhar system will not be narrowly limited to the applications described in Section 7. The Act potentially covers everyone. It can include all the transactions conducted by an individual and the State in relation to benefits and subsidies; and the transactions between an individual and a corporate entity, where the private entity uses the Aadhar number for identification and authentication. The expanded scope of coverage, along with the absence of protecting privacy, implies that this Act has reduced the overall privacy protections enjoyed by residents in India – whether in their interactions with the State to access subsidies/benefits or in their interactions with corporate entities.

Notice

Manner of giving notice left to the realm of regulations

Section 3(2) of the Aadhar Act requires that the agencies enrolling people for distribution of Aadhar numbers should give people notice regarding:

(a) the manner in which the information shall be used;
(b) the nature of recipients with whom the information is intended to be shared during authentication; and

(c) the existence of a right to access information, the procedure for making requests for such access, and details of the person or department in charge to whom such requests can be made.

Section 8(3) of the Aadhaar Act requires that authenticating agencies shall give information to the individuals whose information is to be authenticated regarding

(a) the nature of information that may be shared upon authentication;
(b) the uses to which the information received during authentication may be put by the requesting entity; and
(c) alternatives to submission of identity information to the requesting entity.

It must be noted that the Act leaves the manner of giving such notice in the realm of regulations and does not specify how this notice is to be provided, which leaves important specifics to the realm of the executive. This left an unclear picture as to how comprehensive, accessible, and frequent this notice must be.

No prescription of data breach notification

The Aadhar Act fails to prescribe 'data breach notification' requirements, mandating the UIDAI to inform an individual, the Aadhaar number holder, that their identity (biometric and demographic) information has been shared or used without their knowledge or consent.

Lack of an effective enforcement mechanism

Section 3(2) of the Act require the enrolling agencies to inform the individual about the manner in which their information shall be used and shared and ensure that their identity information is only used for submission to the Central Identities Data Repository.

Section 8(2) (b) and section (3) of the Aadhaar Act. The authenticating entities are allowed to use the identity information only for the purpose of submission to the CIDR for authentication. Further, Section 29(3) (a) of the Act specifies that identity information available to a requesting entity shall not be used for any purpose other than that specified to the individual at the time of submitting the information for authentication.

Section 41 imposes a penalty on the requesting entity for non-compliance.

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 authentication entity which uses the information for any purpose not already specified will be liable to a punishment of imprisonment of up to 3 years or a fine of Rs. 10,000/- or both. In a case of companies, the maximum fine amount would be increased to Rs. 1000000/.

The lack of an effective enforcement mechanism undermines these provisions. The Act does not detail how an Aadhaar number holder can escalate the issue (since only the UIDAI can file a complaint) or what standard will be used to determine whether the requesting entity has provided the information in a

clear and suitable 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 reveal identity information, authentication records or any information in the CIDR following a court order by a District Judge or higher. Any such order may only be made after UIDAI is allowed to appear in a hearing. According to section 33 of the Act, the confidentiality provisions in Sections 28 and 29 will not apply with respect to disclosure made in the interest of national security following directions by a Joint Secretary to the Government of India, or an officer of a higher rank, authorised for this purpose.

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

The provisions regulating disclosure of private information under the act differ from guidelines specified under the. The Act differs from guidelines for phone tapping in two ways. First, the act permits sharing in the interest of 'national security' rather than for public emergency or public safety. Second, the order can be issued by an officer of the rank of Joint Secretary, instead of a home secretary.[55]

Sweeping exception of National Securit

Section 33(2) carves out an express exception to Section 29(1)(b)'s stipulation of "using" core biometric information for any purpose other than generation of Aadhaar numbers and authentication under this Act if it is in the interest of `national security'. The phrase "national security" is undefined in the Act, as well as the General Clauses Act, and thus the circumstances in which an individual's information may be disclosed remains open to interpretation, therefore, section 33 is very vague.

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

Section 33(2) makes an exception to the security, confidentiality and disclosure provisions on the direction of the Joint Secretary in the interest of national security. Such a direction has to be reviewed by a three-member 'Oversight Committee', consisting of the Cabinet Secretary, the Secretary of the Department of Legal Affairs and the Secretary of the Department of Electronics and Information Technology. The second proviso further provides that such a direction shall be valid for three months, after which it can be reviewed and extended every three months. This is problematic for various reasons.

Since the entire process of review of the disclosing order is being handled within the executive and there is no independent oversight. There are no substantive provisions laid down that shall act as the guiding principles for such oversight mechanisms[56].

Lack of defined functions and responsibilities of oversight mechanisms

Section 33 currently specifies a procedure for oversight by a committee, however, there are no substantive provisions laid down as the guiding principles establishing the responsibilities and powers of the oversight mechanism.

Lack of opportunity to data subject

The proviso in section 33(1) only requires a hearing to be given to the UIDAI, and not to the Aadhaar card holder, whose information is being disclosed and in case of a court order identification information and authentication records of an individual can be revealed without any notice or opportunity of hearing to the individual affected. The act does not provide any means by which an individual can contest such an order or challenge it after it has been passed.

Involvement of private entity in the maintenance and establishment of the CIDR

Section 10 of the Act stipulates that the Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations.

[55] PRS Legislative Research, Nine issues to debate on aadhaar Bill (Mar. 11, 2016, 01:39 PM IST), http://www.thehindu.com/news/national/nine-issues-to-debate-on-aadhaar-bill/article8341611.ece.

[56] Amber Sinha, Sumandro Chattapadhayay, Sunil Abraham and Vanya Rakesh, List of Recommendation on the Aadhaar Bill, 2016- Letter Submitted to the Members of Parliament (Mar. 16, 2016), http://cis-india.org/internet-governance/blog/list-of-recommendations-on-the-aadhaar-bill-2016.

If a private entity is involved in the maintenance and establishment of the CIDR it can be presumed that there is the possibility that they would, to some degree, have access to the information stored in the CIDR, yet there are no clear standards in the Act regarding this potential access and the process for appointing such entities. The fact that the UIDAI has been given the freedom to appoint an outside entity to maintain a sensitive asset such as the CIDR raises security concerns.

Conflict of Interest

Courts cannot take cognizance of any offence punishable under the Act unless a complaint is made by the UID authority or a person authorised by it. It is unlike UID will complain against itself in the case of a breach.

Failure of the aadhaar

As per the official data put up on the Telangana government's website, the authentication failure rate for Aadhar-based transactions was at 36% for the period between January to till date; this was higher than the failure rate of 34% recorded in the October-December period last year. In fact, the failure rates in the two districts of Adilabad and Wanarapathy were as high as 46% and 38% respectively in the period between 1 January and 6 April. The Aadhar biometric authentication failure rate in the ambitious rural job guarantee scheme is as high as 36% in Telangana, data collated by the state government shows. The main reason for the payment failure in the operation of the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) was the biometric mismatch, the data showed. Due to wear and tear of their fingers, rural labourers have failed the biometric authentication. And since iris scanners, largely because they are expensive, have not been deployed widely, workers have been denied wage payments due to them. This failure rate is really very worrisome because it is hurting the livelihood of the people. In the case of ATMs, the failure rate is only 0.5%. But for Aadhar authentication for MGNREGA wages and social security pensions, the failure rate is as high as 30%. 22% of PDS cardholders in Andhra Pradesh could not collect their rations because of fingerprint authentication failure in 290 of the 790 cardholders, and in 93 instances there was an ID mismatch. A recent paper in the Economic and Political Weekly by Hans Mathews, a mathematician with the CIS, shows the programme would fail to uniquely identify individuals in a country of 1.2 billion. This essentially shows that problem is with the Aadhar technology especially when it comes to biometric mismatches.[57]

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 various 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. [58] 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

[57] Prerna Kapoor, Remya Nair and Elizabeth Roche, Aadhaar fails MGNREGS test in Telangana (Apr. 07, 2017, 12:36 AM IST), http://www.livemint.com/Politics/Uf5B33ZB2sYKpmLqwMke8O/Aadhaar-fails-MGNREGS-test-in-Telangana.html.

[58] Anil Padmanbham, Aadhaar in the eye of the privacy storm (Apr. 10, 2017, 03:50 AM IST), http://www.livemint.com/Opinion/AF15Svbru1pCvHwV8AYDPP/Aadhaar-In-the-eye-of-the-privacy-storm.html?li_source=LI&li_medium=news_rec.

procedural safeguard measures for the security of the data and the privacy of the citizens to remove all these lacunae.[59] 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 way to make it completely safe. In this complex and evolving technology errors are inevitable. For instance, across its products, Google has to manage around 2 billion lines of source code. The average program has 14 separate vulnerabilities, each of them a potential of illicit entry. Such weaknesses are compounded by the history of the Internet, in which security was an afterthought. 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.[60]

The right to Privacy is not 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.[61] Numerous checks and balances need to be put in place for ensuring the security and stability of the Aadhaar ecosystem. This is not just important from the point of view of individuals, even companies and countries are vulnerable (hackers mostly go after institutions, which curate all kinds of information).[62]

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.

.

[59]Vrinda Bhandari and Renuka Sane, Analysing the Information Technology Act (2000) from the viewpoint of protecting privacy (Mar. 18, 2016, 12:19 PM IST), https://ajayshahblog.blogspot.nl/2016/03/analysing-information-technology-act.html.

[60]Anil Padmanabhan, Aadhaar: in the eye of the privacy storm, Live Mint (Apr. 10, 2017, 03: 50 AM IST), http://www.livemint.com/Opinion/AF15Svbru1pCvHwV8AYDPP/Aadhaar-In-the-eye-of-the-privacy-storm.html?li_source=LI&li_medium=news_rec.

[61] Apurva Vishwanath, Govt defends to link PAN with Aadhaar in Supreme Court, Live Mint (May 02, 2017, 01:49 PM IST), http://www.livemint.com/Politics/k5RPTacEjeUEyLPidgIvtO/Govt-defends-decision-to-link-PAN-with-Aadhaar-in-Supreme-Co.html.

[62] Anil Padmanabhan, Aadhaar: in the eye of the privacy storm, Live Mint (Apr. 10, 2017, 03: 50 AM IST), http://www.livemint.com/Opinion/AF15Svbru1pCvHwV8AYDPP/Aadhaar-In-the-eye-of-the-privacy-storm.html?li_source=LI&li_medium=news_rec.