Analysis of Aadhar Card : Issues and Recommendations

Avishi Chopra

TABLE OF CONTENTS

INTRODUCTION

On January 28 2009, following a notification by the Planning Commission, the UIDAI was established. The UID number, often known as Aadhaar, was created to eliminate fraudulent or duplicate identities. The first UID, a 12-digit unique number (authenticated digitally), was generated in September 2010. Since then, the government has issued more than 129 Crore Aadhaars until March 2021. Today, Aadhaar is used by several government ministries and departments, as well as other institutions such as banks and mobile providers, to verify the identity of applicants. Before the Aadhaar system, the Union and State governments ran into a significant stumbling problem while implementing various assistance schemes: identifying the proper people, particularly the intended recipients. Even the lack of a legitimate and authenticated identification document hampered the implementation and delivery of different government social programmes. Citizens were needed to provide many documents as proof of identity to various government and private entities, including passports, driver's licence, and ration cards, among others, making it cumbersome for them, particularly those who did not have any of these identity credentials. Hence, the Aadhar system was introduced in India to do away with such issues[1].

TIMELINE OF THE UNIQUE IDENTIFICATION SYSTEM IN INDIA

- (03 March 2006) - Administrative approval for the project "Unique ID for BPL families" was given by the erstwhile Department of Information Technology (DIT), Ministry of Communications and Information Technology.

- (03 July 2006)- A Process Committee was set up to suggest procedures for updating, modifying, adding and deleting data fields from the core database under the Unique ID for the BPL families' project.

- (30 August 2007)- The Process Committee decided to furnish a detailed proposal based on the resource model for seeking "in principle" approval from the erstwhile Planning Commission.

- (28 January 2009)- Unique Identification Authority of India was created.

[1] https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html

- (September 2010)- The first UID was generated by a digital identity platform set up by UIDAI with the brand name ‘Aadhaar’.
- (29 September 2010)- The ambitious Aadhaar Scheme was launched in Tembhli- a village in the Nandurbar district of Maharashtra, where the first Aadhaar was issued.

- (March 2021) The Aadhaar database has since reached 129.04 Crore and is considered one of the largest biometric-based identification systems in the world.

Background Of Aadhar And Verdict Of Supreme Court

In 2010, then-Prime Minister Manmohan Singh and then-Congress President Sonia Gandhi announced Aadhaar. In September 2013, the Supreme Court began the first hearing of what was to become a series of Aadhaar petitions. The petition's purpose was to look at the utility of the Aadhaar card.

In less than two weeks, the court concluded that the lack of an Aadhaar card did not justify depriving them of any benefit or service. In response to the ruling, then-Minister of Petroleum and Natural Gas Veerappa Moily, stated that the Aadhaar-linked Direct Benefit Transfer (DBT) scheme for subsidised LPG supply would continue and that the government would petition the Supreme Court for a "correction" of the judgement.

The Union Cabinet approved the National Identification Authority of India Bill in October, giving the UIDAI a legislative standing. Shortly after, the UIDAI presented a massive list of petitioners in favour of the Aadhaar programme before the Supreme Court.

Narendra Modi chose to examine the development of the Aadhaar project after assuming power in 2014. He considered the prospect of leveraging the platform to restart the Direct Benefit Transfer of subsidised schemes. The government proposed making Aadhaar mandatory for various services in the coming months, including passports (though it quickly backtracked), PAN cards, and Jan Dhan accounts, but the Supreme Court was sceptical. Ultimately, the Centre concluded that Aadhaar was not mandatory for public services.

In March 2016, the government tabled the contentious Aadhaar bill in Parliament as a money bill. Opposition parties have accused the administration of using the money bill to circumvent the Rajya Sabha, where the BJP does not have a majority.

The law, however, did pass in the Lok Sabha, which Arvind Panagariya applauded. While the Congress, which held a majority in the Rajya Sabha, returned the bill with five revisions, the BJP refused to accept them and approved the bill. Arun Jaitley, speaking on the subject, stated that privacy is not an 'absolute' right. In the Fall of 2017, the court consented to hear a challenge on the constitutionality of the Aadhaar Act and set up a 5-judge bench to hear all petitions on the programme[2].

When the BJP was in opposition, leading members of the party constantly attacked Aadhaar, branding it a fraud scheme and raising concerns about its security. The BJP raised the red flag against the Congress-led UPA's UIDAI bill, which attempted to give statutory backing to the Unique Identity programme. However, after assuming power, the NDA administration introduced a revised Aadhaar Bill as a money bill to escape a veto by the opposition-dominated Rajya Sabha[3].

Section 7 of the Aadhaar Act deals with the targeted distribution of financial and other subsidies, benefits, and services financed by the Indian Consolidated Fund. In addition, the Government added a new clause permitting states to use Aadhaar data to implement their initiatives. The Supreme Court, on the other hand, barred private businesses from using individual Aadhaar numbers to determine the identity of the individual concerned for any reason according to a contract, citing a violation of the fundamental right to privacy.

[2] https://www.deccanherald.com/national/aadhaar-act-verdict-history-693614.html

[3] https://www.hindustantimes.com/india-news/aadhaar-flip-flop-when-the-bjp-called-it-a-fraud-scheme-aimed-at-legalising-illegal-immigrants/story-tRxUVr8qTDbPHwInD7m3tN.html

Private entities were not allowed to utilise Aadhaar numbers for authentication unless they had a contract with the individual involved. This restriction would permit private companies to profit from an individual's biometric and demographic data, while effectively precluding businesses from using Aadhaar-based e-KYC to verify an individual's identification, formerly the primary method through which many businesses met the applicable 'know your customer' (KYC) requirements.

The Aadhaar Act, 2016 does not violate the fundamental right to privacy. Section 7 of the Act is constitutional. 'Benefits' and 'services' should be those which have the colour of some subsidies, namely welfare schemes of the Government whereby the Government is doling out such benefits which are targeted at a particular deprived class[4]. No deserving person would be denied the benefit of a scheme on the failure of authentication, and it would be appropriate to make a suitable provision for establishing an identity by alternate means. No child should be denied the benefit of any of the welfare schemes covered under Section 7 if, for some reason, she/he is not able to produce the Aadhaar number, and the benefit shall be given by verifying the identity based on any other document.

A variety of legislation, circulars, and orders requiring the mandatory linking of Aadhaar for receiving relevant services were also decided by the Supreme Court. The Supreme Court ruled that the phrase "for any purpose" was comprehensive and prone to abuse. The Supreme Court ruled that the goal must be "lawfully supported."

Even the prospect of collecting and using Aadhaar numbers for authentication as part of a contract was rejected because it could force people to give their agreement in the form of a contract for an unlawful purpose. According to the Supreme Court, the contract must be "supported by law," according to the Supreme Court.

Additionally, residents were entitled to obtain an Aadhaar number but such an enrolment was voluntary. However, for those who wished to seek or receive any subsidy, benefit or services under the welfare schemes of the Government, the enrollment was mandatory. As such CBSE, NEET, JEE, UGC etc. could not make the requirement of Aadhaar mandatory for the students.

[4] https://www.livemint.com/politics/policy/aadhaar-amendments-new-clause-to-allow-use-of-aadhaar-data-for-state-schemes-1562782722324.html

The characterization of the bill incorporated many of the progressive data protection concepts inspired by the European Union General Data Protection Regulations, was also considered in the verdict (the "EU GDPR").

The obligation to link Aadhaar numbers to PANs was legal and appropriate because it was based on a statute and served a legitimate governmental objective. Failing the proportionality test, the obligation to link Aadhaar number to bank account was deemed invalid. The proportionality test can be assessed on the following -

(a)The action must be legally sanctioned;

(b) the proposed action must be essential for a legitimate goal in a democratic society;

(c) the magnitude of such interference must be proportional to the necessity for it;

(d) Procedural safeguards must be in place to prevent such intervention from being abused[5].

The need to link Aadhaar numbers to mobile numbers was invalid since it did not serve a legitimate state goal and encroached on individual liberty disproportionately.

On 25 May 2022, The Supreme Court ordered the UIDAI to issue Aadhaar cards to sex workers without requiring them to show proof of residence.Under the Constitution, sex workers have the same right to dignity, decency, and privacy as other workers. It has directed the issuance of Aadhar cards to sex workers based on proforma certificate issued by UIDAI and has to be submitted by a gazetted officer at the Nation AIDS Control Organization or the project director of the state[6].

SCHEMES LINKED TO AADHAR CARD

The goal of the Aadhaar Act, which was introduced as a Money Bill and passed by the Lok Sabha, is to "allow for targeted delivery of subsidies and services to people residing in India by assigning them unique identity numbers, termed Aadhaar numbers." However, the Supreme Court has not made it

[5] https://www.barandbench.com/columns/proportionality-test-for-aadhaar-the-supreme-courts-two-approaches

[6] https://economictimes.indiatimes.com/news/india/provide-aadhaar-cards-to-sex-workers-without-home-proof-sc-tells-uidai/articleshow/91797480.cms?from=mdr

"mandatory." However, being linked to over 50 schemes like government financial benefits and subsidies, including LPG subsidies, government scholarships, provident funds, pensions, food security, and other bank payments, it is now necessary. Some of the essential schemes are-

- On June 16, 2017, the Centre made citing Aadhaar obligatory for **opening bank accounts** and any financial transaction of $50,000 or more.
- **Direct Benefit Transfer (DBT)**, a system to transfer the subsidy and welfare amount directly to the beneficiary's bank account instead of the traditional practice of giving a banker's cheque or cash, was the first significant implementation of an Aadhaar-based service.
- The Employees Provident Fund Organization assigns a Universal Account Number to make **money transfers** easier when an employee changes jobs. The employee can deposit the PF amount straight to the savings account by linking his or her Aadhaar to this UAN.
- The Modi government's Pradhan Mantri Ujjwala Yojana provides free LPG connections to those living below the poverty line (BPL). Aadhaar is used to validate the beneficiary's claim and transmit the subsidy amount.
- In six Union Territories (UTs), namely Andaman and Nicobar Islands, Chandigarh, Dadra and Nagar Haveli, Daman and Diu, Lakshadweep, and Puducherry, a trial plan for direct delivery of food subsidy under the TPDS was suggested. The Food Corporation of India issues foodgrains at a reasonable cost under the proposed scheme. The difference between the economic cost and the current issue price is credited to the beneficiary's bank account in advance, allowing them to buy food at this price. The requirement of an Aadhar card is not necessary for this scheme. If an Aadhar number is available, it is used at the Fair Price Shop to deduplicate the beneficiary database or verify the **beneficiary's identity.**
- According to the Unique Identification Authority of India (UIDAI), as of November 30, 2012, 18.79 crore Aadhar letters were distributed[7].

PRIVACY AND AADHAR CARD

[7] https://www.thehindu.com/news/national/the-long-list-of-aadhaar-linked-schemes/article17641068.ece

The court supported privacy as a fundamental right, and informational self-determination and an individual's liberty in limiting the use of personal data emerged as significant themes throughout the decision. The **Puttaswamy Judgement** holds that on August 24, 2017, a 9-judge Supreme Court bench gave a unanimous judgement in Justice K.S. Puttaswamy vs. Union of India and several related proceedings upheld that each individual has a fundamental right to privacy under the Indian Constitution[8].

When the Government was pushing linking Aadhaar with various Government schemes and services, leakage of Aadhaar data became a severe issue. This leakage of Aadhaar data has profound implications for individual privacy and national security. The Government confirmed widespread data leakage in a letter to the State Chief Secretaries and the Secretaries dated March 25, 2017. Aadhaar's key privacy issues are-

- Tracking individuals

Individuals can be monitored or placed under surveillance without adequate authorisation or legal sanction utilising authentication and identification records and trails in the Aadhaar database or the databases of one or more authentication-requesting authorities. The location, time, and context of authentication, as well as the services used, may be revealed in these records.

It takes only Rs 500 and 10 minutes to be monitored by a scam "agent". They create a "gateway", provide a login ID and password and pay via Paytm. The risk of obtaining all information of an individual has led to the system of UIDAI (Unique Identification Authority of India), which includes name, address, postal code (PIN), photo, phone number, and email address[9]. Furthermore, The Tribune team paid further Rs 300 to the agent in exchange for "software" that allowed the production of the Aadhaar card after entering any individual's Aadhaar number.

- **Identification without consent**

[8] https://www.scobserver.in/reports/k-s-puttaswamy-right-to-privacy-judgment-of-the-court-in-plain-english-i/

[9] https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361

There remains a high possibility that biometrics may be used illegally to identify people. Identifying people through incorrect matching of fingerprint or iris scans, or facial images recorded in the Aadhaar database, or utilising demographic data to identify people without their knowledge and contravention of legal rules are examples of such infractions.

The following are some ground reports and case studies on how the misuse of privacy is evident.

Eight people were detained in Chandigarh in January 2018 for buying pricey phones with illegal loans guaranteed by bogus Aadhaar cards. The accused, including former bankers and finance firm personnel, allegedly superimposed their images on others' Aadhaar cards to acquire bank loans. They were charged with cheating, fraud, forgery, and criminal conspiracy under the Indian Penal Code.[10]

Around 200 students at Matunga's Institute of Chemical Technology placed their thumbs against thin coatings of a standard resin glue, imprinting them with their fingerprints.Students from Matunga's Institute of Chemical Technology (ICT) used their chemistry skills to break into the institute's biometric attendance system[11].

TRAI Chairman had put out a challenge by making his Aadhar Card public. The hackers claimed to access his private information, including his phone number and e-mail id. This incident raised serious concern and apprehension among the people regarding the safety and security of personal information privacy. The required details for financial transactions, like Card Number, CVV Number, Expiry date, Login Username and Password, are reportedly publicly available. This was a significant threat to the financial security and privacy of the citizens in the country. Some users also posted screenshots of sending one rupee to the account through *Aadhaar*-enabled payment service apps. The ability to send money to a person without his consent could expose someone to blackmail, money laundering and

[10] https://www.business-standard.com/article/economy-policy/from-cheating-banks-to-faking-identity-aadhaar-frauds-peak-in-2018-report-118052300151_1.html

[11] https://www.hindustantimes.com/mumbai-news/you-will-be-glued-to-this-mumbai-college-s-students-trick-biometric-system/story-W64f1jdMtecxKDml2DakeI.html

other dangers. If citizens' privacy and personal information are not secure, it could lead to financial fraud and mental agony. Once revealed, there is an excellent chance of misusing the *Aadhaar* number.

The lack of security against insider threats and the limited use of virtual identities present major privacy problems exacerbated by the lack of an apparent data usage strategy and regulatory monitoring. The privacy risks persist without a necessary permission and purpose limitation framework and a regulatory access control architecture. Inadequate privacy protections could allow the current government enormous access to information and influence over its citizens, jeopardising civil liberty and democracy[12].

DATA PROTECTION BILL

Mr Ravi Shankar Prasad, Minister of Electronics and Information Technology, introduced the Personal Data Protection Bill 2019 in the Lok Sabha on December 11, 2019. The bill aims to secure people's data by establishing a Data Protection Authority.

The bill regulates the processing of personal data by

- The government
- Indian-incorporated firms
- International companies dealing with the personal data of Indian citizens.

Individual rights are outlined in the bill. These rights include the ability to:

1. Obtain confirmation from the fiduciary that their personal data has been processed
2. Request correction of inaccurate, incomplete, or out-of-date personal data,
3. Have personal data transferred to any other data fiduciary in certain circumstances, and
4. Limit the continued disclosure of their personal data by a fiduciary if it is no longer necessary or consent has been withdrawn.

For better service targeting, the central government may direct data fiduciaries to give it with any:

[12] https://www.newindianexpress.com/nation/2018/jul/28/trai-chiefs-personal-details-leaked-after-he-shares-aadhaar-number-in-challenge-to-hackers-1850002.html

(i) Non-personal data

(ii) Anonymized personal data (where the data primary cannot be identified)[13].

Section 35 of the **Personal Data Protection (PDP) Bill** 2019 empowers the Central Government to strike out portions of the aforementioned Act in favour of government agencies, citing "Indian sovereignty and integrity," "public order," and "friendly relations with other nations," and "security of the state."

The UIDAI asked for a blanket exemption from the statutory provision because it already had one under the Aadhar Act. During a meeting with the Joint Parliamentary Committee, UIDAI stated that the two laws (PDP and Aadhar) are counterproductive.

Section 12 of the Act exempts UIDAI from the bill's strictures, allowing it to process data to provide a service or benefit to the data principal. Even in that case, advance notice is required. There could be no duplication of laws because the Aadhaar Act already binds the UIDAI authority. In 2018, the Supreme Court (SC) threw down the Aadhaar Act's national security exception. It indirectly assures that an individual's Aadhaar data is kept private while preventing government access to it[14].

GDPR AND AADHAR

The General Data Protection Regulation (GDPR) is the world's most stringent privacy and security law. Despite the fact that it was designed and passed by the European Union (EU), it imposes duties on organisations anywhere that target or collect data about EU citizens. On May 25, 2018, the regulation went into effect. Those who break the GDPR's privacy and security regulations will face severe fines, with penalties ranging in the tens of millions of euros[15].

[13] https://prsindia.org/billtrack/the-personal-data-protection-bill-2019

[14] https://www.thehindu.com/news/national/uidai-wants-exemption-from-data-protection-bill/article37238680.ece

[15] https://gdpr.eu/what-is-gdpr/

At one end of the scale, Privacy activists consider GDPR to be the pinnacle of privacy protection legislation. Aadhaar, on the other hand, is frequently regarded as the largest villain in India's privacy violation.

Article 85 of the GDPR empowers member states to reconcile the right to personal data protection under the GDPR with the right to freedom of expression and information, including processing for journalistic purposes as well as academic, artistic, and literary purposes, by legislation.

Article 86 refers to the revelation of personal data in official documents stored by a public authority or a private organisation to carry out a public-interest activity under a Right to Information law[16].

AADHAR IN ELECTIONS

The Lok Sabha passed the **Election Laws (Amendment) Bill 2021** that links electoral roll data with Aadhaar cards. Within this law, electoral registration officers can ask for the 12-digit number assigned by UIDAI to register as voters. Authentication and identifying already registered entries also require the Aadhar number.

The law also states that no application would be denied voting in case of inability to authenticate their Aadhar number due to sufficient cause. They would be able to furnish other documents. This amendment would solve the problem of multiple enrolments at different places and lead to better data management. The Bill, according to the opposition, would disenfranchise many voters and would be a violation of the Constitution's right to privacy.According to Congress, this law was to be opposed as Aadhar was only meant to prove residence, not citizenship. However, such an amendment would mean voting by even non-residents[17].

The data of 78 million people were illegally obtained and used to profile voters, according to the Unique Identification Authority of India (UIDAI), which controls Aadhaar. Around the same time, Andhra Pradesh and Telangana removed approximately 5.5 million voters from the electoral rolls after

[16] http://privacy.ind.in/wp/2018/03/17/gdpr-and-aadhaar/

[17] https://timesofindia.indiatimes.com/business/india-business/linking-of-electoral-data-with-aadhaar-all-you-need-to-know/articleshow/88408171.cms

their Aadhaar numbers were connected to voter identity cards without the required door-to-door verification. A large number of voters objected.

Telangana Police's special investigation team (SIT) raided the Hyderabad headquarters of a private company called IT Grids (India) Pvt Ltd and discovered that the company had access to "stolen" voter data and Aadhaar data of over 78 million people in Andhra Pradesh and Telangana. According to the SIT's inquiry report, the company integrated this information to create a mobile application for the then-incumbent Telugu Desam Party (TDP) in Andhra Pradesh, which used it for "voter profiling," "targeted campaigning," and even "voter deletion" during the assembly elections. The voter-profiling scandal went even further in Andhra Pradesh. According to a Telangana police probe, the incumbent TDP was not only utilising Aadhaar and government benefit data to target voters for its assembly election campaign but was also removing citizens who were likely to vote for the opposition from the electoral lists. After Aadhaar and voter-ID data were first linked in Andhra Pradesh that year, around 2.5 million voters were ostensibly purged from the electoral rolls.

According to analysts, the above reports show how Aadhaar-enabled voter-profiling can be utilised by political parties to rig elections[18].

LINKING OF AADHAAR WITH VOTER ID

On December 21, the Rajya Sabha passed a bill that allows Aadhaar to be linked to electoral roll data a day after the Lok Sabha approved it. The Election Laws (Amendment) Bill, 2021, which was likely to have a significant impact on the operation of Indian democracy, was rushed through both Houses without much public debate. The measure aims to eliminate electoral roll duplication and give voters numerous qualifying dates. According to the Union government and the Election Commission of India, the effort was intended to clean up electoral lists by deleting fake voters and duplicate entries and making the voting process more legitimate.

[18] https://www.article-14.com/post/govt-has-cleared-linking-of-aadhaar-voter-data-past-experience-reveals-how-it-can-be-manipulated-61c937a621c09

Election Laws (Amendment) Bill, 2021

- It proposes amending Section 23 of the Representation of Peoples Act, 1950, to allow for the integration of electoral roll data with the Aadhaar ecosystem.
- This was intended to reduce the risk of the same person being enrolled in several places.
- Remote voting would be possible due to seeding Aadhar data with voter identities, which could benefit migrant voters.
- The connection of Aadhar cards was thought to help prevent spurious and fraudulent voting.
- **Concerns about privacy:**

1. Electoral data was then stored in its database by the Election Commission of India (ECI), which was separate from other government databases.
2. The proposed Aadhaar-election database link would make the information available to the ECI and UIDAI. Citizens' privacy may be violated as a result of this.
3. Legitimate voters would be disenfranchised simply because they refuse or cannot give their Aadhaar details.

- Beneficiary Voter Identification: The amendment would lead to political profiling. The government could follow any voter who has used their Aadhaar to get welfare subsidies and benefits far more easily now that electoral IDs are linked to Aadhaar numbers. Political parties could use this information to focus their messaging to specific voters in a way that isn't publicly available[19].

According to opposition leaders, the bill would contradict the Supreme Court's Aadhaar decision and the standards given down in the Puttaswamy decision, which established that the right to privacy is a basic right.

Despite opposition criticism of a bill linking Aadhaar to electoral records, government officials said that the measure would eliminate the "big problem" of multiple enrollments of the same individual at different locations and assist in "clean up" the voter list to a large extent[20].

[19] https://www.drishtiias.com/daily-updates/daily-news-editorials/linking-voter-s-id-with-aadhar-ecosystem

[20] https://www.ndtv.com/india-news/linking-aadhaar-with-voter-id-will-end-multiple-enrollment-says-centre-report-2662552

The National Election Roll Purification and Authentication Programme began seven years ago with the goal of mapping Aadhaar with voter ID cards or EPIC (Electoral Photo ID Card) to 'purify' electoral rolls (NERPAP). It was originally implemented in the Telugu states, commencing with a pilot at Nizamabad and Hyderabad, like with many other technological trials in India. This Telangana experiment was used as a model for a nationwide exercise that began in March 2015 and was halted by the Supreme Court in August that year.

The project's consequences were evident in the Telangana Assembly elections of 2018 when lakhs of voters could not vote because their names were absent from the electoral rolls. According to an RTI response, the Telangana State Election Commission used Aadhaar to delete nearly 30 lakh voters using software designed to detect duplicate entries without conducting proper door-to-door verification or notifying all voters to reapply for voter ID in the event of wrongful deletions[21].

According to detractors, merging Samagra Kutumba Survey (SKS) data with Aadhaar formed a 360-degree profile, which was used to remove voters from 'inconvenient' locations under various voting stations, castes, and socioeconomic groups.

It is unknown how the 30 lakh victims of 2018 were classified. However, critics claim that the SKS, which was nothing more than an exercise to map the profiles and voting behaviour of residents who voted in the first-ever election held after the passage of the Andhra Pradesh Reorganization Act 2014, which paved the way for the creation of Telangana, was at the root of the whole issue[22]. While the Act specifies a detailed method for removing voters from the rolls, there was no application form for the reinstatement of names that had been removed.

There have been numerous exclusions and anomalies in attempts to link Aadhaar to PDS or MGNREGA. According to a 2020 study, when the previous BJP government in Jharkhand pushed for

[21] https://www.thenewsminute.com/article/explained-aadhaar-voter-id-linking-and-major-concerns-over-move-159061

[22] https://thefederal.com/the-eighth-column/why-should-aadhaar-voter-id-not-be-linked-telangana-has-the-answers/

linking Aadhaar to ration cards to eliminate bogus or duplicate cards, nearly 90% of the cards eliminated belonged to legitimate households.

Comprehensive Legislation Required: A free and fair election requires an error-free electoral roll. The government should introduce a thorough bill so that serious debate in Parliament can occur. The bill should also establish the scope of data sharing between the two databases, the mechanisms for obtaining consent, and whether or not consent to link the databases can be rescinded. There should be a proper system to record the information about the stakeholders concerning data sharing. **Citizens' Privacy Protection:** The government must pass the Personal Data Protection (PDP) law before moving further with the Aadhaar-voter ID connection. The PDP framework must also apply to government agencies, requiring them to seek an individual's explicit consent before sharing their information across several government institutions.

DIGITAL INDIA AND AADHAR

Aadhaar has brought the most crucial goal of Digital India to life: digital inclusion and empowerment of ordinary Indians. Data security, privacy, non-duplication, data integrity, and other elements were built into the Aadhaar eco-architecture system. Additionally, security audits were performed. In a multilayer method to provide security measures, many formats were used at different stages, from the point of collection to the end.

UIDAI also received STQC ISO 27001:2013 certification and was designated as a "critical infrastructure" by the National Critical Information Infrastructure Protection Centre (NCIIPC), offering an extra layer of IT security assurance. States/UTs were asked to seed the available Aadhaar numbers of eligible beneficiaries in their ration cards/beneficiaries database so that duplicate ration cards/ineligible beneficiaries might be identified and weeded out of the TPDS and food subsidies can be targeted correctly. At the national level, the Aadhaar numbers of at least one family member were seeded into 85.41 per cent of the total 23.18 crore ration cards. Between 2013 and 2018, a total of 2.98 crore ration cards were reported as deleted/cancelled as a result of the use of technology, de-duplication through digitization, Aadhar seeding, detection of duplicate/ineligible ration cards, beneficiary migration/deaths, change of household economic status, and during the run-up to and implementation of the Ration Card Reform Act[23].

IT Ministry's plan: One digital ID that links to other IDs and can access them (INDEA2.0)

The Ministry of Electronics and Information Technology (MeitY) has proposed a new "Federated Digital Identities" paradigm, in which a citizen's multiple digital IDs, ranging from PAN and Aadhaar to driving licence and passport numbers, can be linked, stored, and accessed through a single unique ID.

The citizen will be "empowered" by the umbrella digital identity, which will "put her in control of various identities and give her the choice of choosing which one to employ for what reason." The Federal Digital Identity appears to be a one-stop-shop for saving federal and state government ID information. If all goes as planned, this digital ID could be used for KYC or eKYC (know your customer) procedures. The planned strategy, which was first presented in 2017, has been dubbed India Enterprise Architecture (IndEA) 2.0, to connect government and commercial organisations to streamline online identification processes[24].

AADHAR ENABLED PAYMENT SYSTEM (AePS)

The India Post Payments Bank (IPPB) has imposed service charges for the Aadhaar Enabled Payment System (AePS). From June 15, 2022, AePS Issuer transaction costs would be in effect.

[23] https://www.hindustantimes.com/analysis/aadhaar-has-built-a-strong-base-for-india-s-digital-achievements/story-FdH9dgLuRF9tM4C9oNp1eJ.html

[24] https://indianexpress.com/article/india/it-ministry-plan-one-digital-id-that-links-7747828/

AePS is a bank-led platform that enables online interoperable financial inclusion transactions at the point of sale (MicroATM) using Aadhaar authentication through any bank's Business correspondent. AePS supports six different types of transactions.

A customer's bank name, Aadhaar number, and biometric obtained during enrolment are the only data required to perform a transaction in this case. Using Aadhaar as an identity to access one's own Aadhaar enabled bank accounts through a Business Correspondent, AEPS was able to perform basic banking transactions such as cash deposit, cash withdrawal, intrabank or interbank fund transfer, account balance, and get a mini statement.

Service fees for IPPB AePS

Each month, the first three AePS issuer operations (cash withdrawal, cash deposit, and mini statement) will be free. AePS issuer cash withdrawals and cash deposits will be charged $20 plus GST for each transaction beyond the free transaction limit. In contrast, mini statement transactions will be charged $5 plus GST per transaction.

Services Provided by AePS

Banking Services

1. Cash Deposit
2. Cash Withdrawl
3. Balance Enquiry
4. Mini Statement
5. Aadhar to Aadhar Fund Transfer
6. Authentication
7. BHIM Aadhar Pay

Other Services

1. eKYC
2. Best Finger Detection
3. Demographic Authentication

4. Tokenization

5. Aadhar Seeding Status[25]

AEPS FRAUD

Aadhaar-enabled payment system (AePS) fraud has reportedly occurred in Telangana.

AePS fraud has been reported in Haryana, Jharkhand, and other regions of the country, prompting the state police to issue a warning. Criminals had stolen biometric data from Haryana's land records website, including thumbprints. They created duplicate prints on silicon and withdrew funds from Aadhaar-linked bank accounts of victims. When people give their biometrics for Aadhaar authentication, they don't know if it is for getting ration or withdrawing money. This information asymmetry results in financial fraud[26].

MISUSE OF AADHAR

The Government of India, Ministry of Electronics & Information Technology released a press on 27 May 2022 regarding the misuse of aadhar and taking caution for the same. They have mentioned using "masked aadhar", which displays only the last four digits of the aadhar number. The government also asked the public to avoid public computers or internet cafes downloading e-Aadhar for precautionary reasons. Only organisations with a user licence from UIDAI can use aadhar to recognize the identity of individuals. Unlicensed private entities can not use aadhar and are considered an offence under Aadhar Act 2016. The Unique Identification Authority of India withdrew this press release that warned people not to share photocopies of their Aadhar cards. Holders of UIDAI-issued Aadhaar cards were only recommended to use and share their UIDAI Aadhaar numbers with caution. The Aadhaar Identity Authentication ecosystem includes enough elements for preserving and safeguarding the Aadhaar holder's identity and privacy.

FLAWS IN THE EXISTING SYSTEM

[25] https://www.livemint.com/news/india/ippb-introduces-service-charges-for-aadhaar-enabled-payment-system-aeps-11653464506366.html

[26] https://timesofindia.indiatimes.com/city/hyderabad/aadhaar-enabled-payment-fraud-on-rise-warn-telangana-cops/articleshow/91877422.cms

A. Verification of the applicants' 'Resident' status

- The UIDAI relied on residents' self-declaration of their 'Resident' status at the time of Aadhaar enrolment, hence the status of Resident or non-Resident remained unverified
- To be eligible for an Aadhaar, an individual must have lived in India for at least 182 days in the twelve months before the date of application, according to the Aadhaar Act.
- However, it was highlighted that the UIDAI regulation did not specify any proof or document for validating the "Resident" criteria in order to qualify as a resident. There is no method for determining the truth of the applicant's testimony

B. Multiple Aadhaar Card Generation

- The de-duplication method remained vulnerable to numerous Aadhaar numbers, necessitating manual intervention to remedy the issue.
- As of November 2019, over 4.75 lakh duplicate Aadhaar numbers had been revoked, according to data from the UIDAI Tech Centre. According to the data, on average, 145 Aadhaars were generated per day during the nine years since 2010, with duplicate numbers requiring revocation.
- To discover duplicate Aadhaars and take corrective action, the UIDAI has implemented a self-cleaning system (an automated procedure). But, residents in Bengaluru RO reported 860 occurrences of multiple Aadhaars in 2018-19, indicating that UIDAI's self-cleaning mechanism was ineffective in detecting and blocking leaks.

C. Minor Children Under the Age of Five Years Enrolment for Aadhaar

- When issuing Aadhaar to minor children under the age of five years, the uniqueness of identity, which is one of its distinguishing features, was not ensured.
- The UID for these children is processed on the basis of demographic information and facial photograph by linking with the UID of any one of the parents.

- These children must update their biometrics (ten fingers, iris, and facial photos) when they turn five and then again when they reach the age of fifteen.
- According to UIDAI regulations, if a kid turns five or fifteen years old and fails to update his or her biometric information within two years of turning that age, his or her Aadhaar number would be cancelled.
- In cases where such update had not been carried out at the expiry of one year after deactivation the Aadhaar number would be omitted.
- Furthermore, UIDAI stated that if an Aadhaar holder enrolled as a kid has reached the age of 15, and his or her biometrics have not been updated, the Aadhaar will be deleted.
- Based on the Supreme Court's ruling that no subsidy, benefits, or services may be refused to a child who did not have an Aadhaar number,issuing cards without biometric authentication to children under the age of five served little purpose given the expenditures involved.

D. Aadhaar Document Management

- All of the Aadhaar numbers maintained in the UIDAI database were not accompanied by documents containing the resident's demographic information, raising questions about the accuracy and completeness of the data acquired and stored by UIDAI prior to 2016.
- Up until July 2016, the Aadhaar Document Management System (ADMS) was responsible for securely storing the physical sets of records submitted by people at the time of enrolment, both in electronic and physical form.
- The ADMS agency collected papers acquired by Enrolment Agencies (EAs) during enrolment/update on a regular basis from EAs for scanning and uploading into a portal. UIDAI ordered online scanning of residents' documents beginning in July 2016, putting an end to the ADMS Agency's document pick-up in June 2017

E. Voluntary Biometric Updates

- The high number of voluntary biometric updates suggested poor biometric capture at enrolment, which resulted in authentication problems, forcing people to update their biometrics.
- A disproportionately high percentage of voluntary biometric upgrades suggested a large volume of authentication failures, requiring Aadhaar number users to update their biometrics. This was also a reflection on the quality of biometric data kept in the CIDR for determining the Aadhaar number holder's uniqueness.
- It was discovered that the UIDAI bears no responsibility for poor biometric capture, and that the burden of updating biometrics is borne by Aadhaar number holders, who must also pay for such updates.

F. Mismanaged Delivery Service

- As seen by the vast number of Aadhaar letters returned as undelivered, UIDAI's arrangements with the Department of Posts were insufficient to ensure delivery of Aadhaar letters to the correct addressee.[27]

RECOMMENDATIONS

Proof Of Residence

[27] file:///C:/Users/Manu/Downloads/24%20of%202021_UIDAI-0624d8136a02d72.65885742%20(3).pdf

In accordance with the terms of the Aadhaar Act, UIDAI may impose a procedure and need proof other than self-declaration to confirm and authenticate applicants' residence status. A resident in economic terms is one whose economic interests are concentrated on the economic territory of the country where he/she lives. Verification of residents apart from self-declaration can be done by analysing the income generation and whether the individual's economic interest lies within the domestic country.

Data Security Preventive Measures

The Aadhaar system is safe in and of itself; however, the third-party websites of government departments that use the Aadhaar data or authentication service are not. Every government website should undergo a thorough security review before deployment. Before using any Aadhaar-related data, SSL, proper access control, regular security assessments, detection and response mechanisms, and so on are all required. To secure the database, both client-side and server-side security should be maintained.

Axis Bank, Suvidhaa Infoserve, and eMadhura used stored biometric information for authentication testing between January 11 and 17, 2017. Hence, it is necessary to implement strong multi-factor authentication.

By continuously weeding out unnecessary data, UIDAI may establish a suitable data archival policy to decrease the risk of data protection vulnerability and prevent saturation of valuable data space owing to redundant and unwanted data.

Management Of Data

Aadhaar cards can be developed into a smart card with a computer chip embedded rather than a piece of paper. This would allow the card to hold personal data independently rather than relying on a centralised government database.

Delivery Service

UIDAI and their logistics partner, DoP, may overcome the delivery issues by creating a bespoke delivery strategy that ensures Aadhaar letters are delivered to the correct addressee.The users must be in the loop of their Aadhar card delivery at every point. Hence, developing a tracking system for the users so that they can keep a check if the location is being reached the right way and a system of “point of contact” so that the user can reach out regarding delivery issues in time before it reaches the wrong address.

Multiple Aadhars

Multiple/duplicate Aadhaar can be prevented by using an identification system inculcating the concept of a foolproof mechanism for capturing unique biometric data.

There are five types of biometric data. To ensure proper biometric verification and prevent duplication, all of the following data can be collected and analysed instead of only finger and iris scanning-

1. Fingerprint scanning-
2. Voice recognition-
3. Iris recognition-
4. Facial recognition-
5. Handwriting recognition- in terms of signature

Aadhar for children

Because uniqueness of identity is the most distinctive element of Aadhaar established through biometrics of the individual, UIDAI may look into other techniques to capture the uniqueness of biometric identity for small children under the age of five.

Voluntary Biometric Updates

The high number of voluntary biometric updates suggested poor biometric capture at enrolment, which resulted in authentication problems, forcing people to update their biometrics.

Biometric updates fall into the following two categories-

- **Mandatory updates-**

1. When a child becomes five years old at the initial enrollment, he or she must supply biometric information. This initial capture is treated as an obligatory update of an existing Aadhaar.
2. When a child is between the ages of five and fifteen at the time of enrollment, they should provide all biometrics for updates when they turn fifteen.

- **Voluntary updates**

1. Accidents or diseases might result in biometric exceptions.
2. Biometric updates resulting from authentication failures (False Rejects - where authentication attempts of a resident with a valid Aadhaar number are refused) caused by faulty biometric capture or poor biometric quality captured during enrolment.
3. You must be at least 15 years old at the time of enrollment. Every ten years, residents are advised to update their biometric data.

Of these biometric updates, mandatory ones are free of cost; however, voluntary updates are chargeable.

Since the voluntary updates due to authentication failure are a problem from UIDAIs side, it should create mechanisms to:

1. Better biometric update in terms of verification-iris, finger scan, handwriting, etc., as discussed earlier, so that voluntary updates due to authentication failures do not occur.
2. However, suppose the authentication failures still occur . In that case, a mechanism should be developed to know why the voluntary biometric update is being.

If the update is being done due to an authentication failure, the fees should not be charged.

IDENTIFICATION SYSTEMS IN OTHER COUNTRIES

MALAYSIA

- MyKad is the country's national identity system. All permanent residents in the country must have a MyKad card, which must be renewed every five years.
- The difference between MyKad and Aadhaar cards is that MyKad is a smart card with a computer chip embedded in it rather than a piece of paper. This allows the card to hold personal data on its own rather than relying on a centralised government database.
- Unlike the Aadhaar card, the user has complete choice over when, when, and how the card is used. This freedom of choice gives the user peace of mind by ensuring that he has control over his personal data. The card can be used for a number of things,such as a digital wallet, driver's licence,ATM card.,etc.
- The card has a feature that can make payments at public places (contactless fund transfer)

GHANA

- The Ghana card, which is comparable to India's Aadhaar card, was created with the goal of delivering government benefits to the public in a quick and painless manner.
- The government maintains a centralised database with all biometric data just like Aadhar in India
- The Ghanaian government also offers services such as biometric verification, personal information verification, and online identity validation to chosen organisations and the people are required to link the aadhar numbers to their bank accounts

BRAZIL

- By using a single card for all identifying purposes, the identity cards are intended to reduce bureaucratic processes and improve citizen convenience. It also serves as proof of citizenship, which the Aadhaar card does not.
- It intends to eliminate the card system entirely, relying solely on fingerprint authentication for services like cash withdrawals from ATMs.
- Fingerprint authentication is similar to the Aadhaar Pay app, which is used by rural Indian retailers. Users can use their fingerprints to authenticate bank transactions using only a biometric fingerprint scanner and their cellphones with this software.

INDONESIA

- Karta Tanda Penduduk is the national identity card of this Southeast Asian country (KTP). There are two versions of this card: a basic version and an electronic version (eKTP).‘
- The Indonesian government intends to make eKTP a requirement for participation in all of its programmes. In Indonesia, a person cannot receive a SIM card without eKTP, just as the telecom authority in India has made linking phone numbers with Aadhaar mandatory.

GERMANY

- On November 1, 2010, the electronic ID card was introduced in Germany .
- Unlike the other ID cards, it is the same size as a check card or bank card and includes a contactless chip (radio frequency chip). The RF chip also saves the information printed on the electronic ID card.

ITALY

- The 2016 Electronic Identity Card is a personal identification document that confirms the holder's identity and may be used to authenticate online government services.
- Its goal is to improve and streamline communication between the government and citizens.

CONCLUSION

Aadhaar, India's unique identification programme, was envisioned as a voluntary identity system for the country's people. The UIDAI was established to test the project and develop appropriate strategies and plans.UIDAI was found to have generated Aadhaar numbers with incomplete holder information/documents, non-establishment of the residency status of applicants with proper documents, non-review/matching of resident documents with the Aadhar database, and acceptance of low-quality biometrics resulting in multiple/duplicate Aadhaar numbers to the same individual. Aadhaar numbers with low-quality biometrics cause authentication errors.UIDAI takes no responsibility for it and instead places the burden of upgrading biometrics on the resident, who is also charged a fee. The costs to the government of issuing Bal-Aadhar numbers could have also been avoided.

UIDAI has asked for an exemption from the Personal Data Protection Bill. As per the PDP Bill, the central government can exempt its agencies from the act's provisions for protecting interests, public order and security, etc.

The Ministry of Electronics and Information Technology (MeitY) has proposed a new "Federated Digital Identities" paradigm, in which a citizen's multiple digital IDs, ranging from PAN and Aadhaar to driving licence and passport numbers, can be linked, stored, and accessed through a single unique ID. UIDAI needs to implement better data protection procedures.