**IN THE SUPREME COURT OF INDIA**
**CIVIL ORIGINAL JURISDICTION**
**WRIT PETITION (CIVIL) NO. 1058 of 2017**

**IN THE MATTER OF:**

**Mathew Thomas** **…Petitioner**

**VERSUS**

**Union of India & Ors** **…Respondents**

# NOTE OF ARGUMENTS BY MR. ANAND GROVER, SENIOR COUNSEL, ON BEHALF OF THE PETITIONER

## Table of Contents:

## I. Aadhaar Project extends far beyond the scope of the Aadhaar Act, and violates Article 21 without the support or sanction of law

1. Right from its inception, the Aadhaar Project has been operated by the State as a vehicle for myriad objectives, many of which go far beyond the mere provision of benefits, subsidies and services – which is the stated object under the Aadhaar Act. Examples of such illegal overreach by the Aadhaar Project are discussed in detail below; these instances directly vitiate the privacy of Aadhaar holders and therefore violate Article 21 of the Constitution, without the sanction of law.

2. The fundamental problem with the Aadhaar Project was noted during its initial stages itself, by the Parliamentary Standing Committee on Finance in its Report on "The National Identification Authority of India Bill, 2010", wherein it was stated that: "*The UID scheme has been conceptualised with no clarity of purpose and leaving many things to be sorted out during the course of its implementation; and is being implemented in a directionless way with a lot of confusion*. *The scheme which was initially meant for BPL families has been extended for all residents in India and to certain other persons.*" See paragraph 3(a) of the Report of the 42nd Parliamentary Standing Committee on Finance on 'The National Identification Authority of India Bill, 2010', in **Petitioner's Vol. I**, **Annexure-1, running page 10.**

3. Between 2010 and 2016, Aadhaar has been used to serve myriad objectives; apart from delivering benefits, these include resident profiling by States, serving of national security interests, enabling new commercial ventures etc. However, few of these purposes were subsequently covered within the ambit of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter "Aadhaar Act"). Thus, the Aadhaar Act and the regulations thereunder extend to only a small part of the overall Aadhaar project.

4. This indicates a fundamental divergence between the existing Aadhaar regulatory framework and the applications of the Aadhaar Project, wherein the Aadhaar Project is utilized for purposes that are either ***currently prohibited*** or ***unregulated*** by the Aadhaar Act. Moreover, this divergence is facilitated on a technological level that is not envisaged

by the Aadhaar regulatory framework. Examples of this divergence are discussed in detail below.

**(A) Unauthorised and Excessive Data Collection – *Illegal Collection of Personal Data***

5. Under the Aadhaar Act, the Unique Identification Authority of India (UIDAI) is empowered only to collect biometric information and demographic information from an Indian resident, both of which are clearly defined under the Aadhaar Act. There is no authority granted under the Aadhaar Act or the corresponding Regulations, to collect any additional information during the enrolment process. In this regard reference is made to Section 2(m) (*definition of enrolment*) of the Aadhaar Act, and Regulations 3 and 4 of the Aadhaar (Enrolment and Update) Regulations 2016 (hereafter "Enrolment Regulations").

6. Accordingly, the only fields of data pertaining to an Indian resident, that may be collected during the Aadhaar enrolment are:

(i) Name
(ii) Date of birth
(iii) Gender
(iv) Address
(v) Email
(vi) Mobile
(vii) Details of Introducer / Head of Family, where such enrolment is carried out

7. Yet, the UIDAI has consistently facilitated the collection of additional information, over and above what is authorized under the Aadhaar Act. This additional data ("Know Your Resident +" or "KYR+") has been collected and illegally shared with third parties, such as the State Resident Data Hubs. A tabular representation of authorised and unauthorised data collection during the Aadhaar enrolment process is appended below; further, a diagram representing the scope of Aadhaar project beyond the Aadhaar Act is annexed at Petitioner's **Volume I** as **Annexure-2**, running **page 17**.

| Permitted Demographic Data under Aadhaar (Enrolment and Updated) Regulations 2016 (Reg.4) | Additional Data Collection facilitated by UIDAI in Kerala | Additional Data Collection facilitated by UIDAI in Karnataka |
|---|---|---|
| Name | Marital Status | Details of any social security pensions availed |
| Date of Birth | Caste Category | Details of Ration Card |
| Gender | Educational Details | Details of NREGA registration |
| Residential Address | Home Ownership Details | Details of any benefits under Bhagya Lakshmi Scheme |
| Mobile Number | Physical Handicap Status | Details of Irrigation Pumpset owned |
| Email Address | Occupation | Details of membership in milk co-operative society |
| Introducer Name | Driving License Number | Details of LPG Connection |
| Introducer Aadhaar Number | Voter ID Card No. | |
| Head of Family Name | PAN Card No. | |
| Relationship | Bank A/c Details | |
| Head of Family Aadhaar Number | LPG Gas Connection Details | |
| One modality of biometric information of Head of Family | Ration Card Number | |
| | Employment Exchange Registration No. | |
| | NREGA Registration No. | |
| | Passport No. | |
| | Comprehensive Health Insurance Scheme Reg. No. | |

8. While such KYR+ data may be collected by the Registrar or the enrolling agency from the resident seeking to enrol for an Aadhaar number, it is the UIDAI that facilitates such collection through the framework, processes and technology provided to the Registrars, which directly enables the collection, storage and transfer of the excessive KYR+ data. The architecture of the enrolment software provided by the UIDAI is specifically designed to permit such capture of data and subsequent transfer.

9. The Registrars are provided with specific encryption keys to access all of this data by the UIDAI – this was confirmed by the Minister of State for Parliamentary Affairs and Planning, Mr. Rajeev Shukla, in the Rajya Sabha on 08.08.2013, when in answer to a question on the enrolment process of Aadhaar, he stated that, "*as soon as the enrolment process in respect of an individual is completed, the data captured by the enrolment agency is encrypted and stored in digitally encrypted format. This data can subsequently be accessed only by using a Private digital key of the UIDAI or Registrars (if Registrars have opted for a copy)*". A copy of the aforesaid response in the Rajya Sabha by the

Minister of State for Parliamentary Affairs and Planning is attached in Petitioner's **Volume I** as **Annexure 3**, running **page 18**.

10. In many instances, such KYR+ data includes information pertaining to sensitive aspects of identity which are specifically prohibited from being included demographic information under the Section 2(k) of the Aadhaar Act and Regulation 4(6) of the Enrolment Regulations. Such KYR+ data differs from State to State, and in several instances includes:

    (i) Information relating to caste;

    (ii) Financial information, such as home ownership, occupation, BPL status etc.;

    (iii) Information relating to education;

    A copy of the Aadhaar enrolment form used in the State of Kerala and KYR+ form used during enrolment in the State of Karnataka are annexed in Petitioner's **Vol I** as **Annexures 4** and **5**, running **pages 19 – 22**.

11. While the collected KYR+ data is not stored directly in the Central Identities Data Repository (CIDR), its very collection and subsequent usage / transfer represents a misuse of the Aadhaar enrolment process and the Aadhaar Project, and indicates a function of the Aadhaar eco-system that is contrary to the provisions of the Aadhaar Act and Regulations. It is further to be noted that, in many cases, KYR+ data also included retention of biometric information.

**(B) State Resident Data Hubs – Illegal Sharing of Aadhaar Data**

12. From its very inception, demographic and biometric information of residents (collectively, "Aadhaar Identity Information") collected at the stage of enrolment was made available to State Governments for their private and unregulated usage. In fact, the UIDAI itself developed the application framework for the various State Resident Data Hub (SRDH) projects across different States, and put in place the mechanism for the transfer of Aadhaar Identity Information (i.e. the biometric and demographic data of an Aadhaar holder – S.2(n) of the Aadhaar Act) to these SRDHs. This is seen in the UIDAI's 'Institutional Framework Document for SRDHs' in **Petitioner's Vol. I** at **Annexure-6 at paragraph 1.1, running page 28** and **paragraph 2.2.1, running page 29.**

13. The setting up of SRDH was facilitated by providing access to the information identity submitted during the enrolment process to the Registrars, which are entities appointed by the UIDAI for the purpose of enrolling Indian residents under the Aadhaar Act. A majority of Registrars are State Governments. Other entities that may be appointed as Registrars are enlisted in Regulation 21 of the Enrolment Regulations. These Registrars retained the Aadhaar Identity Information, thereby creating multiple locations where sensitive personal data of applicants for Aadhaar number was stored apart from the CIDR. Such local storage of Aadhaar Identity Information is disclosed in several manuals and handbooks issued by the UIDAI. In this regard reference is made to Point no. 5 & 6 of the the UIDAI's 'Registrar On-Boarding Process Manual', August 2010 available in **Petitioner's Vol. I Annexure-7 running pages 33-34 of** and the UIDAI's 'Aadhaar Handbook for Registrars', January 2013, annexed at **Petitioner's Vol. I Annexure-8 running page 39**.

14. It is submitted that diversion of Identity Information from the Aadhaar system to alternate databases is not permitted under the Aadhaar Act. In some instances, the Registrars use enrolment forms that have a provision for indicating consent of the Aadhaar applicant for sharing of data collected with entities other than the UIDAI; however, such consent is infirm, given that it has no legislative backing and is invariably not informed. Further, the possession of Identity Information by various Registrars and enrolling agencies appointed under them represents a huge risk to the security of the personal information of Aadhaar enrollees.

15. Further, it is submitted that various state resident data hubs combine such Aadhaar data with data on factors such as health, caste, religion, tribe and financial specifics – thereby creating an alternate version of the CIDR with data that is specifically prohibited in the Aadhaar Act. In this context, reference is made to the following disclosures pertaining to the SRDHs of the following states:

    (i) The website of the SRDH in Odisha states that "*SRDH is a repository of UIDAI data of residents, along with their demographic data and photograph*." Further, Odisha's SRDH project enables the government to inter alia, "*utilize Aadhaar numbers to uniquely identify citizens and the beneficiaries of different schemes implemented by Government*", and "*provide Governments with accurate data on*

*residents, enable direct benefits programs, and allow government departments to coordinate investments and share information*."

Thus, the privacy and confidentiality of Aadhaar Identity Information is being compromised and data is being shared by the Odisha Government using the SRDH.

(ii) Press note released by the Department of Public Relations for the Union Territory of Chandigarh on January 13, 2014, wherein it is stated that the SRDH can "identify beneficiaries for various government schemes like social security pension schemes, slum rehabilitation schemes, scholarship schemes and public distribution system". Additionally, it is also stated that the SRDH "*paves the way for accurate identification of the beneficiary at the time of disbursal of the benefits, later followed by* ***multiple perspectives of analysis*** *such as the distribution, the pattern of use, the comparison of eligibility criteria across multiple schemes, etc., of beneficiaries*".

This is the very definition of profiling, wherein the State aggregates all available data on residents and creates a digital biography.

(iii) The website of the SRDH of Andhra Pradesh, wherein it is claimed that "*the SRDH paves the way for… **multiple perspectives of analysis** such as the distribution, the pattern of use, the comparison of eligibility criteria across multiple schemes, etc., of beneficiaries. SRDH is a complete portal which hosts services as: data management, data search and analytics*".

Screenshots and documents on the above-mentioned SRDH of Odisha, Chandigarh and Andhra Pradesh are annexed in **Petitioner's Vol. I** as **Annexure-9, running page 40**.

16. Further, the Maharashtra Government has engaged a private corporation, SAS, which is headquartered in the United States, to **run analytics** on its SRDH and match 42 million records of Aadhaar with 70 million records of state election data, thereby populating them with the Aadhaar numbers. Details of the SAS Project undertaken by the Maharashtra Government, as disclosed on the eMaharashtra web portal, are annexed at **Petitioner's**

**Vol. I Annexure-10, running page 46**. Such seeding of Aadhaar numbers without consent of the respective users in various databases has been described as "inorganic seeding" by the Respondents.

17. Further, such diversion of Identity Information directly violates the obligation on UIDAI to ensure security and confidentiality of Identity Information under Section 28 of the Aadhaar Act. It is submitted that the entire system of the State Resident Data Hubs is made possible purely on account of the infrastructure built and provided by the UIDAI.

18. A pertinent fact of concern is that the Aadhaar Identity Information is now stored in various different locations, some of which are not adequately regulated by law. This includes the CIDR, SRDH, Registrars and Enrolling Agencies, Requesting Entities etc.

19. This is another illustration of how the Aadhaar project extends far beyond the Aadhaar Act.

20. On February 22, 2018, the UIDAI claimed in court that all biometric data with third parties, such as the SRDH and Registrars, had been deleted. However, there is no evidence for the same – and the permanent deletion of data is not a simple process that can occur with the click of a button. In many instances, physical destruction of servers and hard-drives has to be done, to ensure that such data is not later recovered and put to unauthorized use. A parallel may be drawn to the UK experience of destroying citizen information: when the UK National ID Card Project was abandoned, an observer was appointed to oversee the destruction of the collected data and the entire process was appropriately audited by an independent body. In its affidavit dated 09.03.2018, the Respondent No. 3, the UIDAI has claimed that the Registrars and State Governments have destroyed all 'biometric data' collected during the Aadhaar enrolment vide Registrar packets. It is pertinent to note here that: (a) the destruction of such 'Registrar packets' was self-certified, and (b) there is no word on the destruction of 'biometric' OR 'demographic' data within the SRDH. 'Registrar packets' are merely the vehicle through which such Aadhaar Identity Information was made available to the State Government, and its destruction has no bearing on the various other copies that might have been stored in other locations, including the SRDH. The UIDAI must be called upon to provide evidence of the destruction of the biometric data contained within the SRDH.

### (C) Aggregation of Data within the CIDR – Illegal Storage of Data

21. Under the Aadhaar Act, the CIDR (by definition) is permitted to contain only the following types of information:
    (i) Aadhaar Number (Section 2(h) of the Aadhaar Act)
    (ii) Biometric data (Section 2(h) of the Aadhaar Act)
    (iii) Demographic data (Section 2(h) of the Aadhaar Act)
    (iv) *Information related to the abovementioned* (Section 2(h) of the Aadhaar Act)
    (v) Authentication records (Section 32(1) of the Aadhaar Act, and Regulation 26 of the Authentication Regulations)
    (vi) Meta data (Regulation 26 of the Authentication Regulations)
    (vii) Authentication server side configurations (Regulation 26 of the Authentication Regulations)

22. However, in a Strategy Document released by the UIDAI in 2016, it is disclosed that the CIDR also contained 'aggregations of transaction records' of Aadhaar number holders, after removing personally identifiable information; see **Petitioner's Vol. I** at **Annexure-11**, running **pages 52-53**. The term 'transactions aggregated records' is undefined within the document, and could refer to the aggregation of transactions that are authenticated by Aadhaar number holder. The transactions refer to all of the various Aadhaar authentications made by an Aadhaar holder, whenever he used his Aadhaar number to avail a notified service from the State or a private player. The sum of an Aadhaar number holder's transactions could reveal extremely relevant and detailed information about one's life, such as how many times he visited a hospital, how many times he availed of welfare services, how many times he travelled by aircraft etc. Even if personally identifiable information is removed (i.e. the data is anonymised), the aggregation of data pertaining to an individual is extremely dangerous. The storage of such aggregated data, and even the aggregation of transaction records within the CIDR, is not authorised under the Aadhaar Act. ***Such aggregation also permits profiling*** of Aadhaar holders, where the transaction records aggregated pertain specifically to certain Aadhaar holders.

23. For instance, a 2011 study conducted on the possibility of determining private user information from anonymised location data extracted from call records, showed that the publication of anonymised location data obtained through phone records could lead to a significant privacy risk, and even identification of individuals if combined with any other external data. The aforesaid study authored by Hui Zang and Jean Bolot, titled '*Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study'*, is annexed in **Petitioner's Vol. I** at **Annexure-12**, **running page 54**.

24. Thus, anonymised data can always be reverse engineered or combined with other information and used to track someone. Modern day analytics tools have shown how anonymised data sets can often be combined with publicly available information to reveal exact identities. To illustrate, a recent study conducted in the United States, which sought to propose standards of anonymization necessary for the adequate protection of data, showed how an anonymised medical database, when used in conjunction with a publicly available voter list, made it possible to extract the health records of the Governor of Massachusetts. The aforesaid study authored by L. Sweeney, titled '*k-Anonymity: A Model for Protecting Privacy'*, is attached in **Petitioner's Vol. I** as **Annexure-13, running page 66**. There is no information as to what kind of 'anonymisation' model is followed with regard to 'Transaction Aggregated Records' held within the CIDR, and the mere redaction of 'personally identifiable information' such Name or Address is entirely insufficient to protect the identity of an Aadhaar holder.

25. Moreover, the authentication records of an Aadhaar number holder contains information pertaining to different kinds of authentications conducted within a specific region or PIN Code, and this data could be aggregated to determine the following:
    (i) Authentications performed by a requesting entity registered under the National Tuberculosis Control Program, by individuals within a certain PIN Code; *this discloses health information of a group of individuals within that region*;
    (ii) Number of beneficiaries of various schemes of the National Scheduled Castes Finance and Development Corporation within a certain PIN Code; *this discloses caste based information of a group of individuals within that region.*

26. This indicates that information relating to health and caste could very well be aggregated and stored within the CIDR, which is in direct violation of the prohibition on storage of sensitive data in Regulation 4(6) of the Aadhaar Enrolment Regulations.

27. The aggregation of data in this manner within the CIDR is not permitted under the Aadhaar Act. This is unconnected to the objectives of the Act enshrined in Section 7, and infringes the privacy of individuals (even if personally identifiable information is removed).

28. Accordingly, such aggregation and storage of unauthorised data within the CIDR represents yet another instance of dissonance between the Aadhaar Act and the Aadhaar system.

29. It must be noted here that even the use of the term 'meta data' in Regulation 26 of the Authentication Regulations is *ultra vires* the Aadhaar Act. Meta data, per the Oxford English dictionary and common technical parlance, means "data about other data". It can include virtually anything about a transaction or an individual. Given that there is only one express restriction within the Aadhaar Act on the term 'meta data' – i.e. the restriction on storing the underlying 'purpose of an authentication', under Section 32(3) of the Aadhaar Act – the scope for the storage of other information falling within the ambit of the 'meta data' is unlimited. This could include the IP address of a transaction / authentication, the location of a transaction, the nature of a transaction without specifically capturing purpose (such as visit to a hospital without identifying the purpose of the visit), etc.

30. However, the Aadhaar Act does not use the term 'meta data'. Further, the Aadhaar Act clearly defines the kinds of data that will be stored in the CIDR – which is the Aadhaar number demographic data, biometric data and authentication records. Additional information, such as a record of updation of demographic or biometric data, or issuance of a new Aadhaar number etc., may also be stored, since it is clearly related to the aforesaid. The Aadhaar Act does not leave any scope for the storage of any other type of data within the CIDR. Hence, when there is already clear de-lineation of the permitted data fields within the CIDR, the introduction in the regulations of an all-encompassing

term such as meta data, is an attempt by the UIDAI to introduce a loophole by which other data can be collected and stored.

**(D) Access to the CIDR is in contravention of the Aadhaar Act – Illegal Access of Data**

31. Under the Aadhaar Act, access to the information held within the CIDR is restricted. This is in the interests of keeping the Aadhaar Identity Information safe and confidential, which is a statutory obligation on the UIDAI.

32. Accordingly, there are only three instances in the Aadhaar Act under which the Aadhaar Identity Information (excluding core biometrics) of a person may be accessed:
    (i) By the Aadhaar holder under Section 32(2);
    (ii) Pursuant to the order of a court not inferior to a District Judge under Section 33(1) of the Aadhaar Act;
    (iii) Pursuant to the direction of an officer not below the rank of Joint Secretary to the Government of India, in the interests of national security, provided such direction is reviewed by the Oversight Committee as provided under Section 33(2) of the Aadhaar Act.

33. However, there have been numerous instances of unauthorised third parties being provided with unfettered access to the demographic information within the CIDR, by virtue of the very architecture of the Aadhaar Project.

34. A prime example of this is the access to Aadhaar demographic data provided to enrolment operators, which is *ultra vires* the Aadhaar Act. According to the recent expose conducted by the journalist Rachna Khaira and reported in the Tribune on January 4, 2018, Aadhaar enrolment operators (including lakhs of village-level enterprise (VLE) operators) engaged across the country were able to access, download and print the Aadhaar demographic data of any registered Aadhaar number holder. Access to this functionality was being further sold to third parties for as little as Rs.500. See **Petitioner's Vol. I Annexure-14, running page 80**, for a copy of the FIR filed in the aforesaid 'Tribune expose' incident.

35. Proof of such access for enrolment operators also exists in the User Manual / Installation Guide document released by the UIDAI pertaining to its enrolment and update software, 'Update Client Lite' (hereafter, "UCL"). In the said document, it is disclosed that the UIDAI developed a feature within the UCL to help those residents who had forgotten their Aadhaar numbers and acknowledgement slip, print an E-Aadhaar copy. The resident in question merely had to provide his / her demographic details to the enrolment operator, who could use this feature with the UCL to search for and retrieve the E-Aadhaar. All it requires is the authentication of the enrolment operator performing the search, after which unfettered access is provided to the entire CIDR database. See **Petitioner's Vol. I Annexure-15**, **running pages 86-90**, for extracts of the User Manual / Installation Guide of the UCL software. Thus, enrolment operators gain the ability to enter the 'Name' of any person and view their demographic data; a power that may – under the Aadhaar Act – be exercised only on the order of a District Court Judge or Joint Secretary.

36. It is pertinent to point out that use of this feature, to identify young children or individuals with memory loss or other mental disabilities, has been admitted to by the Respondents in their common affidavit dated January 16, 2018. Such usage of Aadhaar to identify such persons lacking agency has been touted by the UIDAI as a major 'success story' of the Aadhaar project. Reference is made to the paragraphs 141 – 157 of the Common Affidavit filed by the Respondents before this Hon'ble Court on January 16, 2018. However, such children or persons with mental disabilities were unaware of their names, let alone their Aadhaar numbers, and yet the officials cited in the various stories were able to secure their Aadhaar Identity Information using only their biometrics. This is an absolute violation of the security measures purported in the Aadhaar Act, and proves how the technology facilitates access that is not prohibited under the Aadhaar Act.

37. Such provision of universal access to demographic data to entities like enrolment operators and UIDAI employees, a majority of whom are private contractors engaged by Registrars or the UIDAI, represents a huge threat to the privacy of Aadhaar holders and their personal security, and runs contrary to the scheme of the Aadhaar Act which mandates the security and confidentiality of Aadhaar Identity Information.

## (E) Remote Seeding Facility of Aadhaar – Illegal Sharing and Usage of Aadhaar Data

38. The Aadhaar Act envisages that only one method of establishing the identity of an individual – that through authentication. This is evident from the construction of Section 7 of the Act, which reads as follows:

> "*The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India,* ***require that such individual undergo authentication****, or* ***furnish*** *proof of possession of Aadhaar number*".

The construction of Section 7 provides that the establishment of identity will happen with the individual *undergoing* authentication or *furnishing* proof, both of which are actions dependent entirely on the participation of the individual. This is in line with the idea that identification of an individual must entail the participation of that individual. Identification cannot occur remotely or automatically without such participation from the Aadhaar number holder.

39. Thus, the linking of any database to an Aadhaar number ***has*** to happen with the knowledge, consent and participation of the Aadhaar number holder. However, this is not the case with regard to the underlying Aadhaar system that the UIDAI has built.

40. To aid State Governments with collation of resident data against Aadhaar numbers, the UIDAI has developed a technical tool (called the Seeding Tool) to enable a process by which Aadhaar numbers could be inserted into the service delivery databases of various State service providers. Seeding is the remote insertion of Aadhaar numbers into various State databases, without any form of participation, knowledge or consent from the individual; this is also known as "Inorganic Seeding". See **Petitioner's Vol. I Annexure-16, running page 92**, which is a UIDAI document on 'Remote Seeding of Aadhaar' uploaded on the Government's Public Distribution System (PDS) portal.

41. Simply put – the UIDAI's software tools for such 'remote seeding' read through State databases and on the basis of demographic data matching, tags Aadhaar numbers to the corresponding persons. This service, developed by the UIDAI using the CIDR, is

available to Central and State Government databases, and other public utilities like Banks. The UIDAI has made these tools accessible to various State entities in order to help them achieve the remote linkage of parallel state databases with Aadhaar. Further, the UIDAI even appointed private agencies to facilitate and help State agencies and departments with this process, thereby granting such private agencies with direct and unfettered access to demographic data of Aadhaar holders during the process of seeding. In this regard, the Petitioner places reliance on the UIDAI's list of agencies empanelled for the remote seeding of Aadhaar in State delivery databases, annexed in **Petitioner's Vol. I** at **Annexure-17, running pages 93-99**, and the UIDAI - Standard Protocol Covering the Approach & Process for Seeding Aadhaar Numbers in Service Delivery Databases, June 2015, annexed in **Petitioner's Vol. I Annexure-18, running page 103**.

42. Such remote seeding of State databases, resulting in the linkage of State databases to Aadhaar numbers without the consent or participation of the Aadhaar number holder, is not envisaged by the Aadhaar Act, and amounts to another instance of Aadhaar system being used without sanction of the Aadhaar regulatory framework.

43. Accordingly, there is a fundamental divergence between the Aadhaar Act and the overall Aadhaar Project. The Aadhaar Act does not cover all aspects of the Aadhaar Project, and indeed in many instances does not even contemplate the uses to which the Aadhaar Project have been put to use. In effect, the Aadhaar Act and Aadhaar Project are neither co-extensive nor co-terminus; instead, the technology underlying the Aadhaar Project has a life of its own that continues to operate in a legislative void.

44. Thus, while there is potential for the Aadhaar Act to be misused and thereby result in the violation of fundamental rights, a far greater risk is the misuse of the technology underlying the Aadhaar Project in ways that are not contemplated by the Aadhaar Act.

45. In this respect, it is also submitted that Section 59 of the Act does not save any action that is *ultra vires* the Aadhaar Act. Accordingly, the actions of the UIDAI pertaining to:
    (i) Illegal collection of data;
    (ii) Illegal disclosure of Aadhaar data, through diversion to the SRDH;
    (iii) Illegal aggregation of data within the CIDR;
    (iv) Providing unauthorised access to Aadhaar Identity Information;

(v) Illegal disclosure of Aadhaar data, through 'Seeding' and linking of third party databases;

are all *ultra vires* the Aadhaar Act, and unconstitutional, as they amount to grave violations of the fundamental right to privacy of Aadhaar holders.

46. Therefore, large parts of the Aadhaar Project do not have the sanction of law whatsoever. This violates the right to privacy under Article 21 as the Aadhaar illegally handles both, biometric and demographic data with little regard to protection of privacy. It is submitted that data covered by privacy may be collected only if it is authorised by a supporting and valid law, which is not the case with the Aadhaar Project. Additionally, it must be noted that many aspects of the Aadhaar Project still remain unknown, as the technology does not follow the provisions of the law and extends far beyond it – thus, reading down of the Aadhaar Act and striking down the offending provisions therein will not serve to rein in the Project itself. Instead, the Project as a whole is deserving of and needs to be abandoned.

## II. The use of uncertain and unproven Biometric Technology to establish the identity of Indian residents, amounts to a violation of Article 14 and 21

47. No agency, either governmental or private, has conducted an adequate due diligence on the feasibility of the Aadhaar project, either before or after foisting it on the Indian population. Instead, an expensive experiment was launched (that has cost both lives and money) while ignoring strong evidence that the use of biometrics would not resolve the problems were sought to be addressed in the first place. Further, the findings of studies that UIDAI had itself authorised, were ignored, as well as the recommendations of experts in India and the experiences of international authorities with biometrics. When evidence began to mount against the workability of the Aadhaar project in the field, the State continued to press ahead with the project, while either denying the existence of the problems, trivialising the impact of problems, or promising to find solutions. The work of independent researchers and international organisations who have conducted extensive studies on the capacity of biometric technology and found it to be unworkable for the unique identification of individuals across large populations, were also ignored.

48. Accordingly, it is submitted that the Aadhaar Project reduces the identity of Indian residents to an uncertainty, by basing the entire claim of an individual to their identity and personality on the probabilistic process of a defective algorithm. Such usage of an irrational system to identify individuals and the resulting denial of essential services on the basis of this irrational system, amounts to a violation of Article 14 and Article 21 respectively.

49. In this context, it is pertinent to review a sequence of events that show that the State / UIDAI had clear knowledge of the fact that biometrics are fallible and cannot be used for the unique identification of individuals across a population as large and complex as that of India.

### (A) Lack of Administrative Due Diligence prior to introduction:

50. **September 2009**: UIDAI's **Biometric Standing Committee Report** expressed concerns over the workability of a biometric identification system in India

(i) The UIDAI established set up a Biometrics Standard Committee (hereafter, "**BSC**") to evaluate the workability of a biometric system in India. In December 2009, after analysing the fingerprints of 25,000 people obtained from Delhi, Uttar Pradesh, Odisha and Bihar, the BSC submitted a report titled 'Biometrics Design Standards for UID Applications' ("**BSC Report**"). The findings of the BSC Report impugned the potential of the Aadhaar project to function adequately in India on account of the lack of relevant data. These included the following:

(ii) De-duplication of the magnitude required by the UIDAI has never been implemented in the world, with the best-case scenario so far – involving the use of good quality fingerprints – involved a database of only 50 million. The ability to retain efficiency while dealing with a database of over 1 billion has not been adequately analysed. Accordingly, in the absence of empirical India data, *it is not possible for the BSC to precisely predict the improvement in the accuracy of de-duplication*. Refer to **Petitioner's Vol. I, Annexure-27, running pages 156-157** (point 5).

(iii) Fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in-depth in the Indian context (See **Petitioner's Vol. I, Annexure-27, running page 156**). The entire workability of the Aadhaar system is based on the assumption that the UIDAI can obtain fingerprint quality as good as that seen in developed countries (See **Petitioner's Vol. I, Annexure-27, running page 158**). However, Indian conditions are unique, given that (a) a large number of people employed in manual labour, which normally produces poorer biometric samples, and (b) biometric capture processes in rural and mobile environments are less controllable as compared to environmental conditions in the West. (See **Petitioner's Vol. I, Annexure-27, running page 159**).

(iv) Of the 25,000 fingerprints collected for the purpose of the study, 2-5% of the subjects had missing biometrics, on account of failures caused by poorly designed processes. The enrolment process had many loopholes which prevented it from detecting such omissions. (See **Petitioner's Vol. I, Annexure-27, running page 158**).

(v) The Committee strongly recommended that carefully designed experiments and proper statistical analysis under pilot should be carried out to formally predict the

accuracy of biometric systems for Indian rural, and urban environments (See **Petitioner's Vol. I, Annexure-27, running page 160**). However, this recommendation was not adequately implemented by the UIDAI, and the findings of the few studies that were conducted (and left incomplete) were ignored.

51. **Jan-Feb 2010:** Admission of the lack of knowledge of the application of biometric systems in India, in a Call for the hiring of Biometric Consultants issued by the UIDAI

In a notice issued by the UIDAI inviting applications for hiring biometric consultants, the UIDAI made an admission on the lack of knowledge of the achievable accuracy of biometric systems in India. The notice expressly stated that: "*there is a lack of a sound study that documents the accuracy achievable on Indian demographics (i.e., larger percentage of rural population) and in Indian environmental conditions (i.e., extremely hot and humid climates and facilities without air-conditioning)*." Further, the UIDAI also stated that they hadn't found any credible study assessing achievable accuracy in any of the developing countries and admitted that although the UIDAI had performed some preliminary assessments, it was not sufficient to fully understand the achievable de-duplication accuracy. See **Petitioner's Vol. I, Annexure-28, running page 164** (point 3).

52. **Mar-June 2010:** UID Enrolment Proof of Concept Report, 2010 admitted to failure of biometrics for certain sections of the rural population

(i) The UIDAI conducted a Proof of Concept Report to measure quality of biometric data that could be achieved in rural Indian conditions - 75,000 people were enrolled in the first phase and 60,000 of the same lot were enrolled during the second phase to check de-duplication accuracy (See **Petitioner's Vol. I, Annexure-29, running page 170** (para 1)). According to the report, older people and manual workers took longer to enrol than the rest of the population (See at **Petitioner's Vol. I, Annexure-29, running page 171 (**point 3)), and the capture often had to be attempted four times to ensure good quality fingerprints (See **Petitioner's Vol. I, Annexure-29, running page 174** (point 5)). Accordingly, the error rates with regard to biometrics were found as follows (See **Petitioner's Vol. I, Annexure-29, running pages 175 and 176**):

(a) One or more fingers - 1.2% of the enrolees (a little over 14 million persons in a population of 1.2 billion);

(b) Either or both eyes missing or otherwise not capturable- 0.5% (six million in a population of 1.2 billion);

(c) Missing all 10 fingers and both eyes- 0.01 % (1.2 lakh when in a population of 1.2 billion);

(d) False Positive Identification Rate- 0.0025% (30 thousand for a population of 1.2 billion);

(e) False Negative Identification Rate- 0.5% using two irises (six million in 1.2 billion); 0.25% using ten fingerprints (3 million in 1.2 billion); 0.01 percent using ten fingers and two irises (1.2 lakh in 1.2 billion).

(f) Therefore, the total number of 'failure to enrol', 'false positive' and 'false negative' cases is potentially a minimum of 29.27 million people – according to the UIDAI's own PoC.

(ii) It was significant that such a high amount of errors was evident despite using such a small set of test subjects, on account of the Indian conditions. Moreover, certain categories of Indians in rural areas were specifically excluded from the study on account of the type of work they engaged in, such as tea plantation workers and areca nut growers (see **Petitioner's Vol. I, Annexure-29, running page 173** (point (iii)).

53. **December 2011 -** <u>The **42nd Parliamentary Standing Committee** recommended and advised against the implementation of the Aadhaar Scheme</u>

(i) The 42nd Parliamentary Standing Committee, set up to review the National Identification Authority of India Bill, 2010, specifically made recommendations against the adoption of the Aadhaar Scheme. There were numerous reasons advanced for this recommendation, including national security concerns, differences of opinion between various Ministries and Government departments, international experience with regard to the use of biometrics such as in the UK. Most importantly, with regard to the use of biometrics in Indian conditions, it noted that:

(a) An expert working with the Tata Institute of Social Sciences (Dr. R. Ramakumar, Associate Professor) stated clearly that the biometric system was unworkable in India, on the grounds that "*...it has been proven again and again that in the Indian environment, the failure to enroll with fingerprints is as high as 15% due to the prevalence of a huge population dependent on manual labour*." (See **Petitioner's Vol. I, Annexure-1, running page 4** (point 11)).

(b) The Ministry of Planning admitted that: (a) failure to enroll is a reality, (See **Petitioner's Vol. I, Annexure-1**, **running page 4 (**point 11))**,** (b) no feasibility study had been carried out nor had any committee been setup to study aspects of the UID scheme (See **Petitioner's Vol. I, Annexure-1, running page 5** (point 44)), (c) The frontiers of technology in biometric are being ***tested*** and used in the project. The technical architecture of the UID-scheme is at this point, based on ***high-level*** assumptions." (**See Petitioner's Vol. I, Annexure-1, running page 7, (**point 53).

(c) the Ministry of Planning further admitted that UIDAI is cognizant of the fact that biometric matching by its very nature will suffer inaccuracy. They stated that these accuracy levels are less than 99% and that cannot be a reason for not **attempting** to use the technology (It is pertinent to mention that assuming that the error rate is between 0.8 – 1% that would mean exclusion of 9.6-12 million people). See **Petitioner's Vol. I, Annexure-1**, running **page 8,** points 54-55.

(ii) Accordingly, in the **42nd Parliamentary Standing Committee's Observations/Recommendations** (see **Petitioner's Vol. I, Annexure-1, running pages 9-15**), the was stated the following:

(a) The full or near full coverage of marginalised sections for issuing Aadhaar numbers could not be achieved mainly owing to two reasons viz. (i) the UIDAI not having statistical data relating to them; and (ii) estimated failure of biometrics is expected to be as high as 15% due to a large chunk of population being dependent on manual labour (See **Petitioner's Vol. I, Annexure-1, running page 11** (point 3f);

(b) Despite serious differences of opinion within the Government on the UID scheme, on issues such as the involvement of private agencies in a large scale which could pose a threat to national security, necessity of collection of biometrics etc., the scheme was being implemented in an overbearing manner without regard to legalities and other social consequences (see **Petitioner's Vol. I, Annexure-1, running pages 11-12** (point 4);

(c) That though there are significant differences between the ID systems of other countries and the UID scheme, yet there are lessons from the global experience

to be learnt before proceeding with the implementation of the UID scheme – such as the UK's Identity Cards Project – which the Ministry of Planning has ignored completely. The Committee noted that in the Report of the London School of Economics on the UK project, it was observed that identity systems create a range of new and unforeseen problems that pose a potential danger to public interest and the legal rights of individuals (see **Petitioner's Vol. I, Annexure-1, running page 13** (point 6); and

(d) That no effort was made to study the financial implications of the UID scheme and the comparative costs of the Aadhaar number with various existing alternatives. Further, the Committee strongly disapproved of the manner in which the project was hastily implemented without any feasibility studies on important aspects of the scheme. It further stated that it was unknown whether the Proof of Concept Studies took into consideration that the accuracy levels have to be maintained when the project is implemented on a high scale of enrolment of 1.2 billion people (See **Petitioner's Vol. I, Annexure-1, running pages 14-15** (point 8-10))**.**

54. **January 2012:** UIDAI releases new data on workability of the Aadhaar system:

(i) In **January 2012**, in a report titled "*Role of Biometric Technology in Aadhaar Enrollment*", the UIDAI asserted that the biometric system works and that 8.4 Crores had already been enrolled in the system (See **Petitioner's Vol. I, Annexure-30**, running **page 178** (first paragraph)). This was a departure from the findings of the Parliamentary Standing Committee and the Biometric Standards Committee of the UIDAI. The admitted error rates were (See **Petitioner's Vol. I, Annexure-30** , running **pages 180-181**):

(a) Failure to Enroll (FTE) – Zero. *As a policy, every unique resident can be enrolled. (However, this does not talk about the biometric failure rate but only as a policy of non-refusal to enroll).*

(b) Biometric Failure to Enroll Rate- 0.14 % (1.68 million in a population of 1.2 billion).

(c) False Positive Identification Rate- 0.057% (6.84 lakh in a population of 1.2 billion).

(d) False Negative Identification Rate- 0.035% (4.2 lakh in a population of 1.2 billion). The report admits the possibility of a few thousand duplicate Aadhaar cards being issued.

(e) Therefore, the potential total exclusion amounts to a minimum of 27.4 lakh people, by the UIDAI's own admission. In this regard, please see the analysis conducted by Dr. Hans Verghese Mathew, referred to in Paragraph 60 of these Written Submissions.

(ii) With regard to biometric sample quality, the Report provides the following: (See **Petitioner's Vol. I, Annexure-30** , running **page 183**):

(a) Poor quality fingerprint - 2.9% (34.8 million in a population of 1.2 billion).

(b) Poor quality fingerprint and poor quality irises - 0.23 % (2.76 million in a population of 1.2 billion).

(iii) The UIDAI stated that these errors, which affect the de-duplication system, can be taken care of by improving the process that improves the quality of biometric data – but it did not elaborate on what these processes were or how this could be achieved. Instead, it went ahead with the Aadhaar enrolment without providing any proof that the errors were taken care of, or that the error rate had been sufficiently reduced.

55. **March 2012:** Fingerprint Authentication Report throws further doubt on the workability of Aadhaar

(i) The fingerprint authentication report focused on findings of Proof of Concept studies carried out by the UIDAI from January 2011-January 2012. The report observed that using only the right index finger and the right thumb, which is the traditional authentication procedure did not give the desired accuracy (See **Petitioner's Vol. I, Annexure-31**, running **page 186**), and thereby recommended strategies such as a "Best Finger Detection" step (identification of which fingers would provide better authentication results (**See Petitioner's Vol. I, Annexure-31,** running **page 190** (point 2)), for improving accuracy in authentication. The UIDAI thereby conducted a PoC study on the Best Finger Detection process; the following error rates were noted in the Best Finger Detection Test:

(a) Single Finger Authentication (1 attempt)- 6.5% (78 million in a population of 1.2 billion). (See **Petitioner's Vol. I, Annexure-31** , running **page 187**)

(b) Single Finger Authentication (upto 3 attempts)- 3.5% (42 million in a population of 1.2 billion). (See **Petitioner's Vol. I, Annexure-31** , running **page 187**)

(c) Two Finger Authentication (1 attempt)- 2% (24 million in a population of 1.2 billion). (See **Petitioner's Vol. I, Annexure-31** , running **page 187**)

(d) Two Finger Authentication (upto 3 attempts)- 1% (12 million in a population of 1.2 billion). (**See Petitioner's Vol. I, Annexure-31** , running **page 187**)

(e) Cannot reliably authenticate using fingerprints- approximately 1.9% (22.8 million in a population of 1.2 billion). The report states that this 1.9% was not included in further authentication tests. (**See Petitioner's Vol. I, Annexure-31**, running **page 189)**

(ii) Therefore, it was observed that using two best fingers and more than one attempts would reduce error rate. It was also stated that age further played a factor in accuracy results. Finally, it was suggested that biometric authentication be coupled with OTP and Iris Authentication could provide an alternative authentication method in case fingerprints do not work. ***This throws serious doubts on the overall workability of the Aadhaar system, as a majority of Aadhaar authentication agencies / requesting entities do not possess the technology for multi-modal authentication and rely solely on single fingerprint readers.***

56. **September 2012:** Iris Authentication Study carried out was seriously flawed:

(i) The UIDAI published a report on the use of iris authentication in Aadhaar, which was founded on the assumption that iris quality does not change, and that the iris cannot get worn out with age or use or other factors (**See Petitioner's Vol. I, Annexure-32**, running **page 193** (point 1)).

(ii) However, the assumption on which this study was based was directly contradicted by the work of Professor Kevin Bowyer and Professor Samuel P. Fenker, who tested this theory and concluded that there was clear and consistent evidence of an iris template aging effect that is noticeable at one year, which increases with time. They also stated that after a three year lapse, the False Rejection Rate increases by 153%. (See **Petitioner's Vol. I, Annexure-33** , running **page 194)**

57. **2014**: Admission by the UIDAI that biometric technology is poor and could lead to false matches:

(i) In *Unique Identification Authority of India* v. *CBI* (2014), the UIDAI admitted that the underlying Aadhaar technology could throw up false matches. In a rape case in Goa being investigated by the CBI, the CBI obtained a palm impression of an unknown person from the crime scene. The Investigating Officer filed an application in the Court of the Judicial Magistrate for giving directions to the UIDAI to compare the print with the biometrics in the UIDAI database. The Judicial Magistrate passed an order directing the UIDAI to provide necessary data as sought by the CBI. Thereafter, the UIDAI appealed to the High Court against the said order. It was further submitted on behalf of the UIDAI that CBI's request was not legally tenable **but also technically not possible.** It stated that searching the database using fingerprints with moderate or poor quality would result in **lakhs of false matches**. The HC ordered that the Forensic Scientific Lab be allowed to check the three sets of fingerprints. The UIDAI appealed against this order in the Supreme Court and the Supreme Court vide order dated 24.03.2014 refused access to the database to the CBI. (See **Petitioner's Vol. I, Annexure-34** , running **page 201**)

58. **2011 – 2016:** Denial of the existence of the UIDAI Biometrics Centre of Competence (UBCC):

(i) The UIDAI has consistently provided conflicting evidence of whether or not they had followed through on the proposal to set up a Biometrics Centre of Competence (UBCC) to examine the use of biometrics in India. In **February 2011,** The UIDAI on its website in stated that it is necessary to create a UBCC that focuses on the challenges of the UIDAI scheme. It stated that, "Nature and diversity of India's working population adds another challenge to achieving uniqueness through biometrics features. Like other technology fields such as telecommunication, we do not have experience like developed countries to leverage for designing UIDAI's biometric systems". In **February 2012,** the UIDAI on its website stated that contracts have been awarded in 2011 to NISG and Telsima Communications for setting up of UBCC and hiring of space for UBCC respectively. (See **Petitioner's Vol. I, Annexure-35 and Annexure-36** , running **pages 209-212**)

(ii) In **December 2016,** the Minister of State for Electronic and Information Technology in the Rajya Sabha stated that the UBCC never existed in response to a question by Shri Husain Dalwai, Member of the Parliament. (See **Petitioner's Vol. I, Annexure-37** , running **page 213**)

(iii) Thus, while the status of the UBCC remains unclear, it is evident that the UIDAI was aware of the need of a specialised body to address the challenges resulting from use of biometrics. Yet, it failed to follow through on its decision to constitute such a body – a decision for which no reason has been advanced till date, despite the urgent need for further study and review of the use of biometrics in the Indian context.

59. **January 2018**: Use of facial recognition as an additional authentication factor:

(i) Vide Circular No. 2 of 2018 dated **15.01.2018**, the UIDAI stated that it has decided to enable *facial recognition* as some residents face difficulty by using the existing biometric modalities (See **Petitioner's Vol. I, Annexure-38**, running **page 215** (point 3). The circular states that face authentication must be used only in fusion mode with one or more authentication modes. The introduction of face authentication described in Paragraph 88 of the Counter-Affidavit, is yet another deeply flawed measure taken by the UIDAI, likely to be of little use and yet increase costs to the State dramatically. The facial images taken for a majority of the residents during the Aadhaar enrolment process was captured using a 3-5MP web camera in average lighting conditions; given this, the potential for such technology to be inaccurate is extremely high. This is particularly relevant as the images captured for authentication will in all likelihood have contrasting lighting, different camera quality and differences in the facial appearance of the resident. Moreover, such technology is extremely fallible. To put this in perspective: the technology company Apple built a 3D facial recognition technology on its latest iPhone to power its facial recognition system, which is light years ahead of the technology used by the UIDAI, and yet cyber-security researchers were able to fool the iPhone system using a mask. Thus, use of the facial recognition system as a biometric identifier is likely to throw up a lot of false positives and negatives, and add to the overall uncertainty of the system.

(ii) Further, the serious problems with using face as an authentication mode are well known. A 2009, **New York University study entitled, "Facial Recognition Technology** - A Survey of Policy and Implementation Issues" states that face recognition technology gives poor results when used for identification against existing faces on the file. Even using the best algorithm for face recognition would not have lesser error rate if the quality of the image is poor. The Report also refers to the 2002 study of the NIST Facial Recognition Vendor Test, for the top systems, where it was found that recognition performance degraded at approximately 5% per year (see **Petitioner's Vol. I, Annexure-39**, running **page 226** (right hand column, para 3)).

**(B) Failure of Aadhaar**

60. It is submitted that independent studies point to the inevitable failure of the Aadhaar system. In 2016, **a study by Dr. Hans Varghese Mathews, titled "*Flaws in the UIDAI process*",** published in the Economic and Political Weekly, (February 26, 2016, LI No. 9) uses the data of an experiment on errors rates conducted by the UIDAI itself (published in the 2012 report titled '*The Role of Biometric Technology in Aadhaar Enrollment'*). It states that for the current population of 1.2 billion the expected proportion of duplicands (individuals whose identifiers match) is 1/121, **a ratio which is far too high,** as this translates to approximately **1 crore persons being excluded** from the system**.** (See **Petitioner's Vol. I, Annexure-40**, running **page 227**).

61. Further, according to ***a report of the US National Research Council of the National Academies***, even the best-designed biometric systems are bound to have errors such as false matches and false negatives. A false match is where one person is identified as another person, and a false negative is where a person is unable to authenticate himself. The report further stated that false-match errors increase with the number of required comparisons in a large-scale identification system. As most comparisons are false, increasing the size of the database increases the number of opportunities for a false match (See **Petitioner's Vol. I, Annexure-41**, running **page 242**).

62. The fact that such errors and exclusion would result out of the Aadhaar system was well known throughout the Government establishment. It is submitted that **Section 5** of the Aadhaar Act was inserted for this very reason: ***biometrics do not work for a large proportion of the Indian population***. Section 5 recognises that special measures would be needed for a large number of categories within the population, ranging from women (nearly 50% of the population) to people with disabilities, unskilled labourers and nomadic tribes. Consider just two of the biggest categories covered under this provision:

(i) **Women**: Several studies have shown that often have problems with biometric authentication on account of physiological factors. For instance, in her seminal study on biometrics titled "When Biometrics Fail: Gender, Race, and the Technology of Identity" , Shoshana Magnet notes that: "Asian women had skin so fine that it couldn't reliably be used to record or verify a fingerprint". Moreover, in the Indian context, a large amount of women perform hard domestic labour, causing significant alteration in their fingerprints.

(ii) **Indian residents**: atmospheric and environmental conditions, or harsh labour, changes biometrics unalterably. Thus, homeless people, tribal people, agricultural workers, manual labourers, domestic workers etc. will have problems authenticating themselves because of their changing biometrics.

63. The UIDAI was seemingly aware that such special measures would be required to ensure that Enrolment Failures and Authentication Failures do not cripple the system. Yet, till date, special measures for these groups have not been specified with regard to improving their biometric verifiability. This indicates that the UIDAI is more interested in the "issuance of unique numbers to individuals, but not unique identification".

**(C) Resulting Failure Rates and Aadhaar Exclusions:**

64. All of the data above indicates an obvious fact – that there are likely to be unacceptably high failure rates in the Aadhaar system causing huge exclusions. This has been borne out by the experience over the years. For instance, as stated in the Economic Survey Report, January 2017, the authentication failure rates of Aadhaar noticed in ***Jharkhand***

***was 49%, Gujarat was 6%, and Rajasthan was 37%.*** (**See Petitioner's Vol. I, Annexure-42**, running **page 247** (para 9.76, left hand column)).

65. Further, there are numerous smaller studies conducted by economists, researchers and NGOs that indicate a similarly high rate of exclusion:

    i. Study conducted in 2017 titled "***Accessing the Right to Food in Delhi"*** by Nandini Nayak and Shikha Nehra, published in the Economic and Political Weekly (EPW) (See **Petitioner's Vol. I, Annexure-43**, **running page 248)** reviewed the impact of the Aadhaar on the PDS system on 320 randomly selected households in Delhi. It found that:

        (a) over 20% of the surveyed households had family members deleted from their ration cards on account of lack of an Aadhaar,

        (b) over 23% faced serious problems with Aadhaar authentication when attempting to obtain their PDS entitlements, and

        (c) 62% did not know how or where to file a complaint if they were excluded from obtaining rations upon an authentication failure.

    ii. A 2017 study titled "***Well done ABBA*"** conducted by Somachi, Bej, Pandey on Aadhaar and the Public Distribution System in Hyderabad, published in the EPW **(**See **Petitioner's Vol. I, Annexure-44**, running **page 251)** focussed on a PDS survey of 80 households in Hyderabad. Their findings revealed that 66% faced technological issues with ABBA (Aadhaar-based Biometric Authentication), and over 35% of the households that did not draw their ration entitlement over a month or more were excluded due to Aadhaar failures.

    iii. A 2015 study titled "***FP Shops Left Over Beneficiaries Report: Findings from 5 FP shops***" by the Society for Social Audit, Accountability and Transparency (See **Petitioner's Vol. I, Annexure-45** , running **page 258)** on the experiences of a randomly selected ration shop using Aadhaar authentication from 5 different districts in Andhra Pradesh, found huge proportions of fingerprint authentication failures in each of the instance, which was primarily caused by the nature of occupation of the individual.

iv. A 2017 study titled "***Ten ways MGNREGA Workers Do Not Get Paid***" by Ankita Aggarwal on the experience of the NREGA and Aadhaar, published in the EPW (Vol. 52, Issue No. 6, 11 Feb, 2017) (**See Petitioner's Vol. I, Annexure-46** , running **page 268**), found evidence that suggests that a significant number of Mahatma Gandhi National Rural Employment Guarantee Act workers are not paid for their work, and over 51% of the overall wages were not paid on time. An analysis of such non-payment and delayed payment revealed that the increasing dependence on technology in the implementation of the act is creating new hurdles for wage payments.

66. It must be considered that the consequence of a biometric exclusion in India is not the same as the West, from where such biometric technology – clearly unsuited to Indian conditions – has been imported. In the West, where such technology is used primarily in instances such as office or university attendance systems, or non-welfare based programmes, the impact of exclusion is (at maximum) inconvenience. In India however, the *impact of exclusion on account of the failure of Aadhaar biometric systems, is often death – on account of starvation, denial of essential medical services etc*. At no point has the UIDAI conducted adequate tests to determine whether such a system can be effectively imposed on the Indian population, and till date they have not been able to provide data to support their claim that the Aadhaar system is better than available alternatives and is, in fact, the best option available. Accordingly, the reliance on such an uncertain biometric system makes the entire Aadhaar Project irrational and violative of Article 14 and 21 of the Constitution.

67. Further, the Aadhaar Project violates the principle of 'proportionality'. Given the grievous violations of the fundamental rights of Indian residents resulting from the Aadhaar Project, the Government was duty bound to explore the 'least restrictive' option available to achieving their intended objectives, which was not done. Reference is made to *Om Kumar* v. *Union of India* (2001) 2 SCC 386, wherein it was held that: "*By 'proportionality', we mean the question whether, while regulating exercise of fundamental rights, the appropriate or least restrictive choice of measures has been made by the legislature or the administrator so as to achieve the object of the legislation or the purpose of the administrative order, as the case may be. Under the principle, the Court will see that the legislature and the administrative authority 'maintain a proper balance*

*between the adverse effects which the legislation or the administrative order may have on the rights, liberties or interests of persons keeping in mind the purpose which they were intended to serve'. The legislature and the administrative authority are however given at area of discretion or a range of choices but as to whether the choice made infringes the rights excessively or not is for the Court. That is what is meant by proportionality.*"

68. The Aadhaar Project is not the 'least restrictive choice' available to the State with regard to increasing the efficiency of welfare schemes, as its effect on the right to privacy, the right to life and the right to equality are overly disproportionate. Simple computerisation of all beneficiary data and PDS records had led to significant increases in efficiency and unique identification of beneficiaries. The regular revision of entitlement lists will ensure a significant amount of integrity in PDS, as was shown by the efforts undertaken in this regard after the enactment of the National Food Security Act, 2013. Better accounting and audit processes will ensure that food grains and other resources are not stolen at source or from storage, before it reaches the last mile of the PDS system.

## III. Absolute Lack of Security in the Aadhaar Project amounts to a gross violation of the Right to Privacy under Article 21

### (A) Contracts with Foreign Agencies render the Aadhaar 'insecure ab initio'

69. It is submitted that of the identity information collected under the Aadhaar Project was compromised at the inception. In that sense, the Aadhaar system is a prime example of a technological system being "**Insecure Ab Initio**". It is submitted that Aadhaar system is *insecure ab initio* for the following reasons:

    (i) That foreign corporations were engaged to build the Aadhaar system, giving them complete access to all Aadhaar-information and continuing control over the Aadhaar technology; and

    (ii) That the Aadhaar-data was diverted into non-secure destinations before even it entered the CIDR.

70. The Government of India engaged foreign corporations to act as 'Biometric Service Providers' (hereinafter "BSPs"), who built the underlying technology on which the Aadhaar system now runs. In 2010, at the inception of the Aadhaar project, contracts were awarded to different foreign based BSPs for the 'design, supply and implementation of the biometric solutions to be used by the UIDAI to set up the Aadhaar infrastructure', which included L-1 Identity Solutions Operating Company Private Limited (hereinafter "L-1 India").

71. L-1 is the Indian subsidiary of L-1 Identity Solutions Operating Company (hereinafter "**L-1, US**"), a company incorporated in Delaware, USA. A copy of the contract between L-1 India and the President of India acting through the UIDAI, dated August 24, 2010, sets out the commercial and technical understanding between the UIDAI and L-1 for the development of the Aadhaar system.

72. As per the Contract, L-1 Company was to operate in its capacity of a "Biometric Solution Provider", i.e. it would provide for design, supply and implementation of biometric matching services (**See definition of Biometric Solution Provider, running page 7 of the Petitioner's Vol. III**). Particularly the scope of work under the contract included providing design, supply, install, configure, commission, maintain and support multi-modal Automatic Biometric Identification Subsystem (ABIS), multi-modal software development kit for client enrolment station, verification server, manual adjudication and monitoring function of the UID application (**see clause 1.1 , running page 114 of the Petitioner's Vol III**). The Contract was initially valid for a period of two years or till the completion of 20 crore enrollments, whichever was earlier.

73. Hence, L-1 Company was licensed to provide technological solutions not just at the stage of enrolment, i.e. collection of core biometrics information (finger print and Iris scan), along with demographic details, but also in the process of de-duplication (**See clause 4.1.1 (1), running page 127 of the Petitioner's Vol. III**) and also 1:1 authentication (**See clause 4.1.2, running page 129 of the Petitioner's Vol. III**).

**(i) L-1 Company had access to sensitive personal information of Indian residents**

74. The said contract further discloses that L-1 had access to identity information and related information, of Aadhaar enrollees, and had continuing control over the Aadhaar technology. Further, at the time of signing the contract and during the term of subsistence of the contract there was no applicable law governing the Aadhaar project or data protection. In this context, reference to relevant portions of the contract are made below.

75. Clause 15.1 of Annexure A of the Agreement between the UIDAI and L-1 India (hereinafter "BSP Agreement") states: "*By virtue of this Contract, M/s L-1 Identity Solutions Operating Company may have access to personal information of the Purchaser and/or a third party or any resident of India, any other person covered within the ambit of any legislation as may be applicable. The Purchaser shall have sole ownership of and the right to use, all such data in perpetuity including any data or other information pertaining to the residents of India that may be in the possession of M/s L-1 Identity*

*Solutions Operating Company or the Team of M/s L-1 Identity Solutions Operating Company in the course of performing the Services under this Contract*."
(**See running page 33 of the Petitioner's Vol. III**)

The term 'L-1 Identity Solutions Operating Company', per the recitals of the BSP Agreement, means the United States parent company of L-1 India. The term 'Purchaser', per Clause 1(VII) of Annexure A of the BSP Agreement, means the UIDAI, Government of India.

The term 'Team', per Clause 1(IV) of Annexure A of the BSP Agreement, includes L-1 along with its consortium members, employees of all consortium members, authorized service providers, partners, agents and representatives engaged either directly or indirectly by L-1.

76. From the abovementioned Clause 15.1, it is evident that the L-1 (the US parent company) had access to the personal information of UIDAI, including the Aadhaar data submitted by Indian residents wishing to enroll for Aadhaar. The personal information as mentioned above would include the fingerprint, iris, face photograph and demographic information, or any data such as verifying documents of the nature of passport copy, PAN card copy etc. (**See Clause 3, running page 72 of the Petitioner's Vol. III**). This represents an unacceptable breach of confidentiality and privacy with regard to the intimate data of Indian residents, including biometric data.

77. Further Clause 4.1.1 (1) of Annexure E of the BSP Agreement confirms that L-1 had access to the biometric and demographic data of Aadhaar enrollees. The said provision reads as follows:

***"4.1.1 Multi-modal Biometric de-duplication in the Enrolment Server***
*Considering the expected size of the de-duplication task, the UID enrolment server will utilize:*
*1. Multi-modal de-duplication. Multiple modalities – fingerprint and iris will be used for de-duplication. Face photograph is provided if the vendor desires to use it for de-duplication. While certain demographical information is also provided, UIDAI provides no assurance of its accuracy. Demographic information shall not be used for filtering*

*during the de-duplication process, but this capability shall be preserved for potential implementation in later phases of the UID program. Each multi-model de-duplication request will contain an indexing number (Reference ID) in addition to* ***the multi-modal biometric and demographic data****. In the event one or more duplicate enrolments is found, the ABIS will pass back the Reference ID of the duplicates and the scaled comparison scores upon which the duplicate finding was based. The scaled fusion score returned with each duplicate found will have a range of [0, 100] with 0 indicating the least level of similarity and 100 as the highest level of similarity."*
(**See running page 127 of the Petitioner's Vol. III**)

(i) The term 'de-duplication', per Clause 1(XVIII) of Annexure A of the BSP Agreement, means assurance through biometric comparisons that no enrolled person has been assigned more than one Unique ID number.

(ii) The term 'multi-modal' refers to the different types of biometrics that is collected and processed during Aadhaar enrolment, which in this case includes fingerprints, iris scans and facial photographs.

(iii) The term 'ABIS', per Clause 4 (1) of Annexure E of the BSP Agreement, means Automated Biometric Identification System, which is the software the performs that de-duplication referred to above.

78. Clause 4.1.1 of Annexure E of the BSP Agreement indicates that each de-duplication request contains all of the relevant Aadhaar data, including demographics and biometrics, and therefore the BSP has access to this data to complete the de-duplication task. Such data is not encrypted, but provided in raw form, as the de-duplication process requires unencrypted data in order to facilitate the comparative check as encrypted data cannot be used for de-duplication.

79. This is reinforced by **Clause 9.8.2** of Annexure E of the BSP Agreement, which deals with the 'Data Quality Monitoring and Reporting' obligations of the BSPs (See **Petitioner's Vol. III running page 164**). Per this provision, the BSP is required to continuously monitor the quality of the data, which entails directly analyzing the Aadhaar data in raw form. Reference is made to the second paragraph of the aforementioned clause on page 53 of Annexure E, which states that: *"Data quality of*

*capture would be received with the image. Image would be received in raw form.*" Here, the term image refers to the scanned captured of the biometrics of Aadhaar holders, i.e. fingerprint, iris and facial photograph.

80. This proves beyond doubt that the BSPs had access to the biometric data of the Aadhaar holders in raw form, and the demographic information of all Aadhaar holders.

81. The provision of access to Aadhaar data, to BSPs is further confirmed in Clause 3 of Annexure B of the BSP Agreement, which states that: "*In the course of the Agreement*, *the Biometric Solution Provider may collect, use, transfer, store or otherwise process (collectively, "process") information that pertains to specific individuals and can be linked to them ("personal data"). Biometric Solution Provider warrants that it shall process all personal data in accordance with applicable law and regulation."* (See **Petitioner's Vol. III, running page 76**)

82. This clause confirms that the foreign BSPs had access to personal information gathered from Indian residents under the Aadhaar project. Pertinently, at the time of execution of the BSP Agreement, there was no Aadhaar legislation or data protection legislation in India.

**(ii) That the BSP Agreement allowed the BSPs to retain data for unreasonably long period of time**

83. Clause 15.3 of Annexure A of the BSP Agreement states that:

> "*The Data shall be retained by M/s L-1 Identity Solutions Operating Company for not more than a period of 7 years, as per the Retention Policy of the Government of India or any other policy that the UIDAI may adopt in the future*."

84. Similarly, Clause 14.2 of Annexure A of the BSP Agreement allows retention of any documents arising out of the agreement for a long period of time. The Clause states that:

> "*The Documents shall be retained by L-1 Identity Solutions Operating Company not more than a period of 7 years as per Retention Policy of Government of India or any other policy that UIDAI may adopt in future*"

(See **Petitioner's Vol. III, running page 33**).

85. Clearly, the BSP Agreement allowed the foreign BSP to retain identification information and documents collected during the process of enrolment for 7 long years. This is an unreasonable time period for the retention of such data, given that the BSP Agreement was valid initially only for a period of 2 years or completion of 20 crore enrollment transactions, whichever would have been earlier (**Petitioner's Vol. III running page 5 Clause 7**).

**(iii) The BSP Agreement facilitated access to personal information by allowing local storage of data**

86. It is submitted that the Contract provided for localized storing of the information collected from residents coming for enrolment. That is, the information collected by L-1 Company in its capacity as the Biometric Service provider was not shared with the Central Information Data Repository in real-time. Instead, the enrolling software was to enroll the *"residents in the field and upload the data onto the server in batch mode"*. This implies that the enrolling agencies had to store the biometric and demographic data locally before it was uploaded on the server (see **Petitioner's Vol. III, running page 121 para 1**).

87. Such storage of biometric information of enrollees was facilitated by a reference database. The BSP Agreement provided that each enrolling system- Automated Biometric Authentication System (ABIS), "*shall maintain its own database of indexed biometric references (called reference database) as well as synchronized disaster recovery database at a separate physical location. This reference database is separate from UID database that is outside of ABIS and not accessible to ABIS. All information necessary for ABIS to perform its functions is maintained by ABIS in the reference database*". (**see Petitioner's Vol. III running page 133 para 1; running page 141 Clause 6.2.1.1 (1)**).

88. It is further submitted that the Contract required L-1 Company to maintain a copy of the reference database at a separate location. This clearly indicates that multiple copies of the sensitive private information of Indian residents were available at separate locations. Hence, even if it is argued that the enrolling agencies/systems did not have direct access to the data stored in the central UID database, now known as the CIDR, the BSP Agreement enabled third parties to have access to personal data of enrollees by very provision for a localized reference database.

89. Further, there is nothing in the contract relating to the destruction of the data retained in this manner, and certification of such deletion. It is submitted that even the present Aadhaar Act contains no provision that relates to the data in these databases.

**(iv) Members of the Board of Directors of the BSP were related to Foreign Intelligence Services**

90. It is submitted that some former members of the Board of Directors were a part of the US intelligence agency. For instance, Louis J. Freeh served as a Director of L-1 Identity Solutions Inc. from July 24, 2006 to August 30, 2007. He had previously served as the Director of the Federal Bureau of Investigation from 1993 to 2001. Further, from July 10, 2006 to 2011, Mr. James M. Loy served as a Director of MorphoTrust USA, Inc. He was also served as Deputy Secretary of U.S. Department of Homeland Security from December 4, 2003 to March 2005. Another former director of L-1 Company, George Tenet (who served at L-1 Company from December 2005 to June 29, 2008) was also a former Chief of the Central Intelligence Agency.

91. It is clear that the BSP Agreement indicates that L-1 had access to confidential Aadhaar data. Under the provisions of the USA Patriot Act, 2001 and the Foreign Intelligence Surveillance Act, 1978, the US Government and Intelligence Agencies can legally require a US based corporation to handover information that it either owns or has access to, and this would extend to the Aadhaar data covered in the scope of the BSP Agreement.

92. Further, in 2009, Safran, a French defence conglomerate in which the French Government had a stake, acquired Morpho, a US company that provided biometric service solutions. The UIDAI signed contracts with both L-1 and Morpho in 2010. A few weeks after the execution of the BSP Agreement, L-1 was acquired by Safran and merged with its subsidiary Morpho. Currently, L-1 is owned by an assortment of private equity investors, and operates under the name IDEMIA Identity and Security.

93. Moreover, personnel of the foreign BSPs continue to be employed by the UIDAI as of January 2018, as indicated by the data that is available on the 'attendance.gov.in' portal – which discloses this (See **running pages 273-275** of the **Petitioner's Vol. I**).

94. The Aadhaar technology, and particularly the algorithms used in ABIS and the Aadhaar de-duplication continue to remain an absolute black-box in that neither the UIDAI nor the Government has control over the technology or understands exactly how it works; this is proprietary technology that is merely under a perpetual license to the UIDAI.

95. Hence, given that any data collected during the process of enrolment and/or use of Aadhaar number was:
    (i) Accessible to foreign BSPs through the whole Aadhaar pipeline;
    (ii) Diverted to various State Resident Data Hubs, and Registrar Local Databases, and Enrolling Agency local devices;

the identity information and related data of Aadhaar enrolled Indian residents is "***insecure ab initio***".

### (B) Failure to ensure Security of Private Data violates Article 21

96. **The architecture of the Aadhaar Project is fundamentally insecure**. By its very operational structure, it entails the exposure of sensitive Aadhaar Identity Information to thousands of intermediaries and storage of sensitive Aadhaar Identity Information in multiple different databases, thereby posing a great risk to both the privacy and security of individuals, and national security.

97. Moreover, the UIDAI has not put in place ***sufficient*** safeguards nor has it specified ***adequate*** security policies binding on all entities engaged within the Aadhaar eco-system. Even after the Aadhaar Act came into force, the UIDAI has failed to discharge its duties under Section 23(2)(m) of the Aadhaar Act and Regulation 3(1) of the Data Security Regulations. The security measures introduced as a reaction to breaches and hacks that occurred, failed to have any effect – not only were they inadequate in terms of addressing and resolving the security threats, these measures have not been enforced across the Aadhaar eco-system, thereby leading to repeated instances of hacks and breaches using the same *modus operandi*. Examples of such instances, occurring at every stage of the Aadhaar infrastructure pipeline, are discussed below.

#### (i) Security Issues in Aadhaar Enrolment

98. Enrolment, per Section 2(m) of the Aadhaar Act, is the process by which biometric and demographic data of Indian residents is collected by enrolling agencies for the purpose of issuance of an Aadhaar number to them. Thus, the data in the CIDR, which forms the basis for authentication and identification under the Aadhaar project, is sourced through the enrolment process. If the data captured during enrolment is incorrect, of poor quality or falsified – the entire Aadhaar project itself will be jeopardized, as the biometric authentications will fail. Thus, sanctity of the enrolment process is paramount.

99. However, a majority of enrolments have been and continue to be carried out by Enrolment Agencies, i.e. entities hired by a Registrar or the UIDAI itself to carry out the process of enrolments. A Registrar is an entity appointed by the UIDAI to supervise the

enrolment process, and includes State Governments, Scheduled Banks etc. (See Regulation 21 of the Authentication Regulations).

100. There have been numerous instances of process violations and errors on the part of Enrolment Agencies engaged by the UIDAI/Registrars. In response to a question posed in the Rajya Sabha, the Minister of Electronics and Information Technology disclosed that as of December 2017, 50,000 Enrolment Agencies were blacklisted / suspended on account of generating excessive errors in the enrolment process. The aforesaid response by the Minister of Electronics and Information Technology is annexed in **Petitioner's Vol I, Annexure 19**, **running page 104** paragraph (a) of the Answer).

101. Further, the Aadhaar enrolment process has been hacked at every level – and despite having detailed knowledge of these hacks, the UIDAI failed to address the underlying issues. In this context, there are several instances where Aadhaar enrolment software was hacked and the access parameters of Enrolment Agencies was duplicated, allowing third parties to generate fake Aadhaar enrolments.

(i) One of the primary safeguards in the enrolment process was that the operator engaged by an Enrolment Agency ("Enrolment Operators") would have to verify an enrolment packet (containing the identity information of an Aadhaar applicant) with his own fingerprint; this fingerprint-based verification would confirm that the enrolment packet submitted to the CIDR for Aadhaar generation arrived from a genuine source.

(ii) The UIDAI had knowledge of the fact that fingerprints of Enrolment Operators were being duplicated and used to authenticate fake enrolments. To increase the veracity of the enrolment packets, the UIDAI, on May 27, 2016, introduced an additional level of authentication for operators – Iris Authentication. Thus, to complete an enrolment, the Enrolment Operator was required to validate the enrolment using both his fingerprints, and (additionally) his iris scans.

(iii) However, in September 2017, it came to light that an enrolment fraud was being perpetrated in **Kanpur**, where fraudsters were able to: (a) clone the fingerprint of the Enrolment Operators, (b) access and modify the enrolment software so as

to bypass the iris authentication requirements, and (c) generate fake Aadhaar enrolments. They further sold the enrolment software of the UIDAI, enabling other entities to generate fake Aadhaar enrolments. The Kanpur Police filed an FIR in the matter, arrested 10 persons accused of the crime, and issued a press release detailing how the crime was committed. In a Press Release dealing with the issue, they specifically noted the fact that the entire enrolment apparatus of the UIDAI – from Registrars to Enrolling Agencies to Supervisors to Operators – were not following any of the basic security policies mandated by the UIDAI. A translated copy of the Press Release by Kanpur Police is annexed in **Petitioner's Vol I, Annexure 20**, **running pages 110-111** (paragraph 6).

(iv) Subsequently, the UIDAI claimed to have fixed the vulnerability in their enrolment software that permitted the hackers to override the iris authentication requirement. However, in February 2018, an **Enrolment Agency in Chandigarh** was hacked using exactly the same modus operandi as that of the Kanpur hack: an artificial rubber fingerprint clone of the Enrolment Operators was used to generate fraudulent Aadhaar enrolments. A copy of the FIR filed by the Haryana Police dated 23.02.2018 with regard to the aforesaid Aadhaar enrolment fraud is annexed in **Petitioner's Vol I, Annexure 21, running page 112**.

102. Not only does this impugn the entire process of enrolment and the engagement of private entities to perform enrolment functions, it reinforces the fact that the use of biometrics for any crucial purpose poses a huge security threat. Moreover, it indicates that a significant amount of the data within the CIDR could be false or incorrect. In response to an RTI application, the Ministry of Electronics and Information Technology (hereafter "MEITY") disclosed *a significant amount of false enrolment data had been detected*, caused on account of intentional fraud by Enrolment Operators. Excerpts from MEITY response to the RTI request dated 23.12.2016, regarding complaints received by the UIDAI against enrolment operators is annexed at **Petitioner's Vol I, Annexure 22,** running **page 117**. See particularly **running pages 130** (point no. 614) and **131** (point no. 713) of the **Petitioner's Vol I** in this regard.

**(ii) Security Issues with regard to Aadhaar Authentication**

103. There are several intermediary entities involved in the process of an Aadhaar authentication. This includes:

(i) Authentication Service Agencies (hereafter "ASA"), which are entities operating the secure leased lines through which access to the CIDR is permitted. No authentication access is permitted to the CIDR without going through an ASA.

(ii) Authentication User Agency (hereafter "AUA") which is an entity registered with the UIDAI and granted the ability to make authentication requests to the CIDR, on behalf of an Aadhaar holder. AUAs are also requesting entities, and in response to their authentication requests they can receive either (a) a Y/N response or (b) e-KYC response depending on the nature of their business.

(iii) Sub-AUA, which is an affiliated to an AUA, and accordingly capable of making authentication requests through the AUA. They are also requesting entities.

See **Petitioner's Vol I, Annexure 23**, **running page 149** for a pictorial representation of Aadhaar Authentication Process.

104. The AUA and the Sub-AUA receive biometric and demographic information from the Aadhaar holder, which they use to request authentication from the CIDR through the UIDAI's provided channels. Upon having this information authenticated from the CIDR, they may use the authenticated information received for any purpose that is specified to the Aadhaar holder, and share it with any third party after obtaining consent from the Aadhaar holder. It is to be pointed out herein that the requirement of consent under Section 8 is not checked by the UIDAI, making that safeguard virtually ineffective. This is evidenced by the recent incident of **Bharti Airtel** having opened payment bank accounts based on Aadhaar E-KYC to all subscribers who went to Airtel to link their SIM cards with Aadhaar.

105. Moreover, the scope for misuse of information submitted to a requesting entity is immense. An example is the fraud perpetrated by **Axis Bank, Suvidhaa Infoserve and e-**

**Mudhra** between 14 July 2016 and 19 February 2017, in which UIDAI had filed a complaint with the Cyber Cell of the Delhi Police. The three entities had stored the biometrics of a customer locally, and used this to impersonate the person subsequently and conduct illegal authentications over 8 months. This proves how easily the security of Aadhaar can be compromised by the requesting entity itself, if biometrics are locally stored. The legal prohibition on such activities, contained in Regulation 17 of the Authentication Regulations, is a negligible deterrent – and the technical safeguards are entirely inadequate.

106. In February 2018, the **Delhi** Police filed an FIR for against **a coaching institute** working in tandem with an online lending start-up that was using Aadhaar authentication to sanction loans on behalf of students to the account of the coaching institute. Investigation is on-going, but misuse of Aadhaar technology is apparent – wherein E-Sign facility is being used to defraud unwitting people. It is also worth pointing here that the e-KYC mechanism of sharing of CIDR data with any requesting entity was notably absent in the NIDAI Bill, 2010, which only envisaged a Yes/No authentication response; this the premise on which Aadhaar enrolments were done for long.

107. Given the immense usage of Aadhaar across the board for public and private transactions, there is a ***forced data trail*** of the personal information of Indian residents being left across numerous third party systems, which information poses a serious threat to informational privacy.

108. In response to the frequent storage and abuse of biometrics of Aadhaar holders by requesting entities, the UIDAI introduced the concept of a **'registered device'** in January 2017. The use of only 'registered biometric devices' to perform authentications was intended to prevent the local storage of biometrics and thereby effectively end the problem of *skimming of biometrics* (wherein the biometrics are lifted from impressions left by the Aadhaar holder, or duplicated). In accordance with the notification issued in this regard, no authentications would be permitted from unregistered devices post June 2017. The UIDAI circular dated 31.10.2017 extending timeline for implementation of registered devices for Aadhaar authentication is annexed in **Petitioner's Vol I, Annexure 24** , **running page 150**.

109. Further, the UIDAI has *not stopped* accepting authentication requests from unregistered devices. Instead, they introduced a penalty system, of approximately 20 paise for each authentication request from an unregistered device. This is a small price to pay for violating security norms, and moreover, this cost can easily be passed on to the Aadhaar holder availing of the service from the requesting entity using the unregistered device. Even this penalty has not been imposed till date – reference is made to an NPCI circular disclosing that discussions were on amongst the MEITY, DFS and UIDAI for the waiver of penalties for using unregistered devices for Aadhaar authentication, as of December 28, 2017. A copy of the aforesaid NPCI circular is annexed in **Petitioner's Vol I, Annexure 25**, running **page 151**.

110. Moreover, the Registered Devices specified by the UIDAI rely on remotely accessed software encryption for ensuring security of biometrics, not hardware-level encryption. Thus the security of captured biometrics is minimal, as there is no way that the UIDAI can prevent local storage of biometrics if the biometric device is modified to do so. Much of the problem of local storage of biometrics could have been avoided if the encryption was done at the hardware level of the device.

111. Further, Registered Devices are not individually audited. Instead, devices of a manufacturer whose prototype / samples have been certified by the Standardisation Testing and Quality Certification ("STQC") directorate of the Ministry of Electronics and Information Technology, qualifies as a registered device. Hence requesting entities can continue to subvert the system – particularly since there are no individual audits or on the ground; the UIDAI's security system is a reactive one, and not proactive in terms of conducting active audits and checks on Aadhaar entities.

112. The extent of the problem is further illustrated by the **Aadhaar-PDS fraud instance in Surat** in February 2018. In this instance, the *Civil Supplies Department of the Gujarat Government* had an alternate database of the biometrics of beneficiaries registered for its public distribution system. This was illegally obtained by two fair price shop owners, for a price. The biometrics of all beneficiaries attached to their shop were extracted, and then used to create an electronic record that showed that all entitled beneficiaries had received their rations, when in reality they were siphoned off by the shop owners. An FIR was filed in the matter and is currently under investigation.

113. What this shows is that the entire Aadhaar project is flawed at the level of system concept, architecture and design. Moreover, the use of biometrics will always leave scope for fraud. The *security policies and data protection practices of the UIDAI* are wholly inadequate to ensure the security of the system, and there is no enforcement of security obligations or audits of Aadhaar entities on the ground. In response to a question in the Lok Sabha, on 03.01.2018 the Minister of State for Electronics and Information Technology admitted that *210 government and educational websites had leaked Aadhaar data into the public domain*; yet, no action has been taken against any of the agencies involved. Moreover, data security is vitiated at every stage of the Aadhaar pipeline; each point therein (from AUAs to ASAs to Enrolment Agencies) have been hacked, their access duplicated and used to illegally access and retain Aadhaar data. In this context, it is submitted that the UIDAI has done little to fulfil its obligations under the Aadhaar Act to ensure the security of Aadhaar data. See **Petitioner's Vol IV**, **Annexure** 2, running **page 27**, for the response in the Lok Sabha disclosing the number of websites that have leaked Aadhaar data.

114. The collection of such personal information from Aadhaar holders without ensuring adequate security for the system is in violation of Article 21 of the Constitution. The need for adequate security to protect personal information is an internationally recognised principle. The 'OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (hereafter "OECD Guidelines") contains the Security Safeguards Principle, which specifies that "*personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data*".

115. There are no proper information security safeguards that protect Aadhaar data from unauthorised disclosure. The power to prescribe these security protocols and technology safeguards has been delegated by the Aadhaar Act to the UIDAI (in Section 23(2)(m)), which responsibility has not been discharged as on date, as the Aadhaar (Data Security) Regulations 2016 do not contain any such protocols or safeguards while leaving it to be specified by the UIDAI at a later date.

116. Given that Indian residents are being forced to use Aadhaar for a whole gamut of public and private services, there are numerous entities with the biometrics, demographics and records of the Aadhaar holder. A diagrammatic representation of this data trail is set out in **Petitioner's Vol I, Annexure 26, running page 152**. Considering the vast potential for leakages, the UIDAI should have specified a global technical security policy for each of the entities engaged in the Aadhaar infrastructure pipeline, including Authentication User Agencies, Authentication Service Agencies, Sub-AUAs, etc. The technical devices used by them should have been inspected and certified, and regular audits should have been conducted at random to ensure security – these obligations also find mention in Regulation 21 of the Authentication Regulations. Swift penal action should have been taken against defaulters. Yet, till date, the UIDAI has failed in these obligations – no proof of an eco-system level audit has been provided till data.

117. Effectively, the Aadhaar project did not have sufficient security safeguards, and thus was unfit to collect sensitive and personal data of Indian residents. Not only are the security measures introduced inadequate, they also specifically fail to address insider threats to data security. In paragraph 69 of their Common Affidavit dated 09.03.2018, the Respondents have admitted that security breaches can continue to occur where the operator or agency handling the biometric device is involved – i.e. where insider fraud or collusion occurs. They assert that such a risk is present in non-Aadhaar systems, and hence its presence in Aadhaar-enabled systems should not be impugned. Not only is this a highly flawed argument, it must be noted that over 90% of the Aadhaar Project is carried out through third parties engaged for the purpose, from enrolment to authentication to even remote seeding. To ignore the possibility of fraud from these parties, when the entire Aadhaar project is overly dependent on them, represents a grave oversight by the UIDAI.

118. Additionally, all of the security measures introduced by the UIDAI are in response to specific flaws discovered through breaches and hacking; the security regime of the UIDAI is, therefore, entirely reactive and not pro-active. For example, the 'registered biometric device' stipulations were introduced only after and in response to the Axis Bank – Suvidhaa Infosever – e-Mudhra incident. The newly proposed Virtual ID system, where the Aadhaar number of individuals are masked with a virtual token, was conceptualised only in response to private entities gaining access to and misusing Aadhaar numbers disclosed at the time of authentication. It is important to note that these

measures, while defective in their own right, were introduced at a stage where over 1 billion Indian residents were enrolled for Aadhaar. Such post-facto measures cannot help ensure the confidentiality and security of data that has already been leaked and disclosed.

119. In this context, courts in the United States have consistently held that the lack of sufficient safeguards, or the use of poor technical and operational systems, that seriously compromise the security of data is major factor in balancing interests to determine whether personal information of individuals should be collected. This was specifically laid out in ***United States* v. *Westinghouse Elec. Corp.,*** (638 F.2d 570, 577 (3d Cir. 1980)), in which it was held that in the context of determining whether an intrusion into the zone of privacy was justified, the court "*must engage in the delicate task of weighing competing interests. The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated,* ***the adequacy of safeguards to prevent unauthorised disclosure,*** *the degree of need for access* ***and whether there is an express statutory mandate****, articulated public policy or other recognizable public interest militating toward access.*" See **Petitioner's Vol II**, **Annexure-1**, running **page 10,** para 12.

120. Similarly, in ***Fraternal Order of Police, Lodge No. 5* v. *City of Philadelphia***, (812 F.2d 105 (3d Cir. 1987)), the Court held that the "the adequacy of safeguards to prevent unauthorized disclosure" was one of the "crucial factors in weighing the competing interests," (between privacy and a State interest, in this case). In that case, the court found found "a complete absence" of protections for the confidential personal information that was sought to be collected by the State. With "no statute or regulation that penalizes officials," the court upheld the injunction forbidding the collection of personal information and required the city to "establish written, explicit, and binding rules that contain adequate safeguards against unnecessary disclosure of the confidential information". See **Petitioner's Vol II**, **Annexure-2, running page 26-27**, para 14.

121. The principle in both these cases was laid out in ***Whalen* v. *Roe*** (429 U.S. 589), wherein the US Supreme Court permitted the disclosure of sensitive and personal information solely on account of the presence of specific and adequate and technical

safeguards and security provisions that were laid out under law and implemented. In *Whalen*, the Court described the extensive security procedures required by the statute and regulation, including storage of information in vaults and locked cabinets in secure areas surrounded by alarm fences, limited retention of five years and special computer operating procedures; only a defined and relatively small group of investigators and staff had access [*to the personal information*], and were subject to statutory sanctions for improper disclosure. See **Petitioner's Vol II**, **Annexure-3, running page 34-40**.

122. Further, the very concept of ensuring the data security of a system dependent on biometrics is flawed. This is because biometrics, while private, are not protected as secret information, but instead easily publicly accessibly – iris scans have been accessed through HD camera shots, fingerprints can easily be lifted from impressions that human beings leave everywhere. Thus, ensuring security of such a system is virtually impossible – as has been demonstrated by the breaches discussed above.

123. Thus, it is submitted that the data security of the Aadhaar project is highly inadequate and insufficient, and data breaches and data theft have occurred to such an extent that a majority of, if not all, the Aadhaar data has already been leaked into the public domain. This also makes future security innovations pointless, as the item sought to be protected has already been compromised.

124. In this regard, the Aadhaar Act itself is highly deficient. As established in numerous cases in the jurisprudence of the European Union, the curtailment of fundamental rights of individuals must be done 'in accordance with law'. In *Amann* v. *Switzerland*, the European Court of Human Rights referred to its established case law to hold that "*the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention ... The phrase thus implies – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded...*". Hence, the quality of the law imposing restrictions on fundamental rights is extremely important, and must be infused with sufficient safeguards. This principle finds utterance in Indian jurisprudence as well, in the *Puttaswamy* judgement where it was held that a law placing restrictions on

fundamental rights must be 'just, fair and reasonable'. See **Petitioner's Vol II, Annexure 4, running pages 60-61** (para 56).

125. Further, in *Surikov* v. *Ukraine*, the ECHR held that an interference with the rights of an individual "in accordance with law" (in addition to the parameters mentioned in *Amann* v. *Switzerland* above*)* requires that the law is accompanied by necessary procedural safeguards affording adequate legal protection against arbitrary application of the relevant legal provisions should accompany the said law. Such interference should also be legitimate and be necessary in a democratic society. (**Para 71)**. Moreover, the applicable law must clearly "*provide clear, detailed rules governing the scope and application of the relevant measures; as well as minimum safeguards concerning inter-alia, duration, storage, usage, access of third parties, procedure for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness at each stage of its processing. There are various crucial stages at which data protection issues under Article 8 of the Convention may arise, including during collection, storage, use and communication of data. At each stage, appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments must be put in place in order to justify the necessity of interference"* (**para 74**). See **Petitioner's Vol II, Annexure 5, running page 88**.

126. In the context of the Aadhaar Act, one of the most basic tenets of the 'quality of the law', evidencing that it is 'just, fair and reasonable' would be sufficient security measures, an adequate enforcement mechanism and appropriate penal provisions. However, none of these requirements are met under Section 29(2) read with Regulation 3 of the Aadhaar (Data Security) Regulations, 2016. The lack of security measures has already been discussed above – the Aadhaar Act delegates the function of prescribing security measures to the UIDAI, which has not fulfilled this duty till date. Moreover, the enforcement mechanisms in the Aadhaar Act are highly deficient, particularly since private enforcement of the Aadhaar Act has been excluded. Section 47 of the Aadhaar Act specifies that only only the UIDAI itself can make a complaint under the Aadhaar Act to a court. With regard to the penal provisions, it is submitted that these are entirely insufficient and deficient. Section 37 of the Aadhaar Act, which prescribes the penalty for *inter alia* disclosures of personal data, extends only to intentional violations, thereby

excluding all unintentional violations. This provides safety to the UIDAI itself, given that numerous disclosures and leakages of Aadhaar data have taken place since the inception of the Aadhaar Project, all of which have been described by the UIDAI as 'inadvertent'. Moreover, Section 37 read with Section 47 ensures that the UIDAI is protected from any prosecution for violation of privacy under the Aadhaar Act, thereby giving its employees and agents little incentive to ensure data security. Therefore, the entire construct of the penal provisions in the Aadhaar Act are designed to protect the UIDAI and State agencies involved with the handling of Aadhaar data. An adequate penal provision in these circumstances would have recognised the principle of 'strict liability' in relation to the handling of personal data of Indian residents.

127. Accordingly, it is submitted that neither does the Aadhaar Act meet the standards required with regard to 'quality of law', nor is it 'just, fair and reasonable', on account of which the legislation violates Article 21 of the Constitution.

## IV. Consequences of Aadhaar data being used for other purposes, such as surveillance and administration

128. The personal data of Indian residents cannot be claimed to a public resource, over which the Indian State has ownership or the power to act as a trustee. The concept of informational privacy has been recognised in the *Puttaswamy* judgement (para 66) as an integral part of the right to life and personal liberty under Article 21, and drawing affirmation from India's commitments under the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR). Moreover, as held in *District Registrar and Collector, Hyderabad* v. *Canara Bank* (2005) 1 SCC 496, personal data does not lose its private and confidential nature upon disclosure to a public functionary (or external party), but instead continues without dilution, as privacy is attached to persons and not items or places.

129. Yet, a major problem with the Aadhaar architecture and technology relates to the usage of the personal data collected by the Aadhaar system – which results in the permanent, indelible and irreparable violation of privacy. Further, such personal data is often to put uses that are far beyond the scope for which it was collected, i.e. the identification of individuals for the delivery of welfare benefits; instead, personal data within the Aadhaar system is diverted for various administrative and commercial purposes of the State and private parties, none of which are sanctified by informed consent or appropriate disclosures. Once personal data is collected and stored within the Aadhaar Project, it is impossible to put fetters on its future usage – such data will inevitably find different applications, and different governments and private entities will put it to various uses that serve their interests.

### (A) Purpose Specification and Use Limitation

130. It is for this reason that the "Purpose Specification" and "Use Limitation" principles, in the context of data collection, are so integral to the protection of data.

131. The principle of 'Purpose Specification', per the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) (hereafter, "OECD Guidelines"),

states that: *The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*

132. The principle of 'Use Limitation', per the OECD Guidelines, states that: *Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.* See **Petitioner's Vol II, Annexure 6,** running **page 104**, for the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013).

133. These principles are also enshrined in the:

(i) European Union's General Data Protection Regulation, in Article 5(1)(b) which states that personal data shall be: "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*" ;and

(ii) the United Kingdom's Data Protection Act, 1998, in Part I of Schedule 1, which states that:

*"2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*

*3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*"

**(B) European Union Jurisprudence on Data Collection, Retention and Usage**

134. Jurisprudence in the European Union has recognised the dangers of retention of personal information, followed by usage for unauthorized or new purposes. With regard to the storage of information and how that might amount to serious interference in a citizen's

life, reference is made once more to *Amann* v. *Switzerland* ([2000] ECHR 88), where the European Court of Human Rights ("ECHR"), held that "*In the instant case, the Court notes that a card containing data relating to the applicant's private life was filled in by the Public Prosecutor's Office and stored in the Confederation's card index. In that connection, it points out that it is not for the Court to speculate as to whether the information gathered on the information gathered on the applicant was sensitive or not or as to whether the applicant has been inconvenienced in any way.* ***It is sufficient for it to find that data relating to the private life of an individual were stored by a public authority*** *to conclude that, in the instant case, the creation and storing of the impugned card amounted to an interference within the meaning of Article 8, with the applicant's right to respect for his private life.*" (See Para 70 - **Petitioner's Vol II**, Annexure 4, **running page 64**).

135. The court in the *Amann* case further states that in analyzing whether the interference was in accordance with the law "*not only requires that the impugned measure should have* ***some basis in domestic law, but also refers to the quality of the law in question****, requiring that it should be* ***accessible to the person*** *concerned* ***and foreseeable as to its effects***" (Para 50, **Petitioner's Vol II**, Annexure 4, **running page 59**) [Emphasis supplied]. A rule is *foreseeable only* when *"it is formulated with sufficient precision to enable any individual to regulate his conduct*". (Para 55-56, **Petitioner's Vol II**, Annexure 4, **running page 60**), and needed "*to be sufficiently clear and detailed to afford appropriate protection against interference by the authorities with the applicant's right to respect for his private life and correspondence*." (Para 58, **Petitioner's Vol II**, Annexure 4, **running page 61**). The court further stated that generic principles set out in the law such as "*there must be legal basis for the processing of legal data"* and "*personal data must be processed only for very specific purposes"* fail to indicate the scope and conditions of exercise of such discretion.

136. In this context, it must be stated that the Aadhaar Act provides absolutely no safeguards with regard to the usage of Aadhaar data by the State. The only protection afforded is in Section 28 and 29 of the Aadhaar Act, and even these provide the Executive with the scope to introduce exceptions through delegated legislation. Further, the Aadhaar data is already being used for purposes other than that which it was first collected for – an example of e-KYC, which is commercial application of the information that was collected

for the purpose of facilitating the targeting of beneficiaries of centrally funded welfare schemes.

137. In *Surikov* v. *Ukraine*, the complainant approached the European Court of Human Rights on the grounds that his rights under Article 8(1) of the Charter of Fundamental Rights of the European Union, which provide that '*Everyone has the right to the protection of personal data concerning him or her*', had been violated when his employer had arbitrarily collected, retained and used sensitive data regarding his mental health. The information related to previous service that the complainant had rendered in his country's armed forces, and was wholly unconnected with the complainant's extant employment, and was allegedly used to deny him a promotion. The court applied the following principles in deciding whether these actions affected the complainant's right to protection of personal data:

(i) Whether the rights of the individual were interfered with (in this case, the protection of personal data);
(ii) Whether the interference was in accordance with law;
(iii) Whether the interference pursued a legitimate aim;
(iv) Whether the interference was necessary, in relation to
    (a) the collection and retention of personal information;
    (b) the usage of personal information

In deciding the case, the Court reiterated that "*core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and envisage limited periods of storage... In line with this, the Court considers that delegating to every employer a public function involving retention of sensitive health-related data concerning their employees can only be justified under Article 8 if such retention is accompanied by particularly strong procedural guarantees for ensuring, notably, that such data would be kept strictly confidential, would not be used for any other purpose except that for which it was collected*" (Para 86, **Petitioner's Vol II**, Annexure 5, **running page 92**). Thereby, the court placed limits on the retention of data and the requirement of adequate security during the period of retention.

138. Accordingly, in *Surikov*, the ECHR held that a legislation permitting the storage of sensitive data of an individual "*for a very long term and allowed its disclosure and use for purposes unrelated to the original purpose of its collection*" amounted to "*a*

*disproportionate interference with the applicant's right to respect for private life. It cannot be regarded necessary in a democratic society*" (Para 89, **Petitioner's Vol II, Annexure 5**, **running page 93**.

139. Similarly, the unreasonably long retention of sensitive personal information (in the form of authentication records) in the CIDR, and the absence of any legal and technical safeguards against their usage for other purposes, is highly problematic in the context of the right to privacy of Aadhaar holders.

140. All over the world, a cognisance is arising of the fact that data stored is a ticking time bomb with regard to the life of the person to whom it so pertains. Yet, the Aadhaar Act, while permitting unjustifiably long retention of data, has incomplete and inadequate provisions for the security of data (*a majority of the security protocols and policies required are yet to be specified*), and no express prohibition on the usage of data for other purposes. This requirement of adequate security is also reflected in the OECD Principles of Data Protection – specifically the Security Safeguards Principle, which states that: "*Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*"

141. Moreover, all of the data has been shared, i.e. publicly disclosed. In this context, the unrestricted storage and use data generated within the Aadhaar system, by entities across the board – from the CIDR, to the SRDH, to Registrars and Requesting Entities – must be stopped. This is because such data will always find usage, if not now, then a year from now, or a decade from now, especially since '*function creep*' is an essential element of the Aadhaar Project. 'Function creep' represents the expansion of the objectives of a legislation far beyond the original intent; and the Aadhaar system has been extended to things that are far beyond the stated objective of the Act.

142. There is no prohibition contained within the Aadhaar Act and Regulations on the usage of "authentication records" and "identity information" to create "processed or derivative information". On the contrary, under Section 23(3)(a) of the Aadhaar Act, the UIDAI may enter into contracts with various entities for the '*processing of information*' – a provision overbroad enough to permit this. Moreover, there is no restriction within the

Aadhaar regulatory framework on the sharing or usage of 'processed or derivative information'.

143. Effectively, the UIDAI facilitates the provision to the Central and State Governments of detailed profiles of Indian residents. This is already being undertaken in various State Resident Data Hubs, where 360 degree profiles of citizens are being built up; a fact admitted on the very web portals of these State Resident Data Hubs.

**(C) State Surveillance**

144. The pervasion of the Aadhaar system and personal data collected could lead to surveillance and citizen rating systems of the kind that is now being seen in China. It is pertinent to note how such infrastructure was built up in China. The Chinese government initially permitted corporations to aggregate personal data of their customers and built algorithms that could then *rate the worth of these customers*. As such applications began to get integrated and large technology companies began to dominate every aspect of citizen lives, the 'Social Credit Rating Systems' that these companies ran became all the more pervasive. Access to the ratings of other people are openly available, thereby allowing an entire economy to treat different citizens differently – a form of citizen discrimination that has pervaded their country. The foremost example of this is the Social Credit Rating System run by Alipay, an affiliate of the software giant Alibaba. On account of Alipay being amongst the most pervasive method of payment in China, it has access to a majority of the financial transactions made by a customer. It uses this data, coupled with social media information, to generate a Social Credit Score, which is posted in the public domain. Anyone wishing to interact with another person may check the Social Credit Score before engaging in social interactions, a phenomenon that is now permitting corporates (and the Chinese government) to exercise innate control over the way people behave with each other, an example being that people with high social credit scores do not engage with those having lower credit scores. By manipulating these scores, the owner of the rating system will be able to create new classes of citizens.

145. Once this system had taken hold of the entire country, the State Council of the Central Government in China released an Outline of the Social Credit System Construction Plan (2014-2020), which specifies that such Social Credit Rating Systems would be integrated

into their governance by 2020. This represents the integration of such infrastructure into the central architecture of the State, and would ensure a devastating amount of State control over its citizens. See **Petitioner's Vol II, Annexure 8**, **running page 114**, for the Notification of the State Council of the Central Government in China titled "Outline of the Social Credit System Construction Plan (2014-2020)" (translated version).

**(D) Algorithmic Governance and Aadhaar Data**

146. The making of administrative decisions purely by using algorithms is highly dangerous. It is for this reason that the European Union specifically introduced, in Article 22(1) of the General Data Protection Regulation, a right to challenge governmental decisions taken solely on the basis of data. The provision reads as follows: "*The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."* Yet, innumerable administrative decisions in India are now being made purely on the basis of algorithms functioning under the Aadhaar Act, without providing any recourse to the affected individuals. An example of this is the de-duplication exercise conducted by the Aadhaar systems. De-duplication is the process by which the biometrics of an Aadhaar applicant is compared with all of the existing biometrics stored within the CIDR, to see if that Aadhaar applicant is already enrolled. As discussed in the previous sections, there are numerous instances of de-duplication failing – on account of the inherent fallibility of biometrics – on account of which people are denied an Aadhaar number. Upon a failure to enrol occurring, there is no method of redressal afforded to the affected individual. Instead, for all practical purposes, that individual ceases to have an identity, and becomes non-existent in the eyes of the State. While Regulation 6 of the Aadhaar (Enrolment and Update) Regulations 2016 specify that special provisions shall be made for those individuals who are unable to enrol, no such provisions have been specified till date.

147. Further, it has already been established that Aadhaar data has been dispersed to various State Governments and State agencies, through the State Resident Data Hubs and the Aadhaar Seeding frameworks. The use of Aadhaar data in governance represents a grave potential danger, with regard to the use of intimate profiles of Indian residents in the

discharge of administrative functions of the State. Once the State has obtained such profiles of its residents, it will be able to selectively discriminate in myriad and often undetectable ways. The following examples relating to the allocation of public resources in India show how such algorithmic governance could affect ordinary citizens.

148. Specifically, with regard to the distribution of electricity, there is already a generic profiling of citizens being conducted by our State entities, on the basis of which the supply of electricity is decided. Not everyone within a city or a State experiences the same level and quantity of electricity supply; certain people or entities receive a lion's share while others are often deprived.

(i) Reference in this context is made to the principles applied by the Maharashtra State Electricity Board ("**MSEB**") to the distribution of load shedding. According to these Principles and Protocols of Load Shedding by MSEB (2005), the MSEB engages in an active evaluation of the different needs of various electricity consumers in the State, and prioritises certain classes over others on factors such as *dependence on electricity* and *importance to the nation*. For example, while considering the are Five major categories of electricity consumers in Maharashtra which are required to be catered to, i.e.

(a) Category A: Industries, MIDC areas and Water Works.
(b) Category B: Metropolitan areas.
(c) Category C: Major cities
(d) Category D: Other urban centres
(e) Category E: Rural areas

(ii) The MSEB prioritises 'Category A' because of its economic importance to the nation, and 'Category B' because of its high dependence on electricity; similarly, Category E is not prioritised, because of its 'low dependence on electricity'. In this manner, the rationale for distribution of load shedding is determined and administered across the State.

See **Petitioner's Vol II, Annexure 10**, running **page 134**, for the "Maharashtra State Electricity Board - 'Principles and protocols of load shedding by MSEB, 2005".

149. The same principle has been applied with regard to the consumption of water in India. Taking the example of Maharashtra again, water is diverted to wealthier neighbourhoods and specific regions. The resulting inequality was captured in an 'Indiaspends' report that analysed the distribution of water:

(i) The average resident in Pune consumes five times as much water as the average resident in Latur, the district facing the brunt of the severe drought in the Marathwada region.

(ii) The coastal Konkan region, accounting for just 14% of the State's population, receives over 50% of the water share.

(iii) Sugarcane crops, which is grown on 4% of the State's farmland by the wealthiest farmers, consumes 70% of the water available for irrigation.

See **Petitioner's Vol II, Annexure 11, running page 141**, for the Indiaspends Report on water inequality dated May 31, 2016, (published in The Wire), titled 'How Water Inequality Governs Maharashtra'.

150. The point of this argument is not to impugn the aforesaid method of distribution of public resources. Instead, it is submitted that data and profiling is already being used by the State, in a yet limited and under-developed form, to treat citizens differently. If these administrative tendencies are supplemented by data based on Aadhaar authentication records and demographic data, the bias in distribution of resources would become far more sophisticated and the resulting inequality would be far more pronounced. For example, decisions made by administrators on the basis of Aadhaar data could enable them to further prioritise certain in different situations, giving rise a form of data-enabled preferential administration. An example of such administration would be: a State Electricity Board deciding that on the eve of the CBSE exams, all households with students appearing for the CBSE exam (which has required Aadhaar linkage in the past) will not have to bear the brunt of load shedding, while other households might be required to do so.

151. The fundamental problem in these cases is that the violation of rights by virtue of use of technology is often undetectable, even by the person being affected. If the water of every person in one neighbourhood was withdrawn for extra 10 minutes and diverted to the people in another neighbourhood, neither might be any the wiser. This is what Prof. Lawrence Lessig meant when he stated in his seminal book on law and modern

technology ‘Code’, that when laws are written into self-executing lines of code, there is great risk in the power to determine the technicalities of such coded law being concentrated in few or private hands.

152. It is the Petitioner’s submission that if Aadhaar data is released into the domain of the State for the use of governance, irrespective of whether such governance will be good or bad, it will never be neutral to all citizens. This is in line with the Kranzburg’s First Law, a proposition introduced in a 1986 Presidential Address titled ‘History and Technology’ delivered by Prof. Melvin Kranzburg, which gave rise to ‘Kranzburg’s Laws of Technology’. According to Prof. Kranzburg, ‘technology is neither good nor evil, but it is not neutral’. Thus, the use of Aadhaar data for governance and administration, without strong and far-reaching safeguards, will lead to a serious deterioration of our democracy.

Thus, given that large parts of the Aadhaar Project is beyond the scope of the Act, and there are no procedural security safeguards in the legal framework, Section 7 of the Aadhaar Act under which personal data is collected, is violative of Article 14 and 21 of the Constitution.

## V. Challenges to the Aadhaar Act and Regulations thereunder

### (A) Excessive Delegation of Powers by the Aadhaar Act to the UIDAI

153. The UIDAI has been set up under Section 11 of the Aadhaar Act, 2016 (hereinafter "the Act"). As per the provision, the UIDAI is to be responsible for the processes of enrolment and authentication. However, the Aadhaar Act, 2016 vide various provisions that delegate powers to the UIDAI that are not limited to mere implementation of the Act.

154. Section 2 of the Aadhaar Act lays down the definition of various terminologies used in the Act. Pertinently **Sections 2(g**) and **2(j)** may be pointed out in this regard. Section 2(g) of the Aadhaar Act defines biometric information as "*photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by regulations*". Similarly, Section 2(j) defines core biometric information to mean, "*finger print, Iris scan, or such other biological attribute of an individual as may be specified by regulations*". Section 2(t) provides that the regulations are to be made by the UIDAI.

155. The UIDAI is empowered under **Section 23(2)(a)** and Section **23(2)(b)** to make regulations for specifying demographic information and biometric information required for enrolment and verification thereof.

156. Further, Section **2(t)** read with Section **23(2)(a)** delegates the function of specifying demographic and biometric information required for enrolment and verification thereof to the UIDAI.

157. The object of the Act is inter alia the targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India. This is done by the Act's provision of allowing 'identification' by verifying biometric information, such as photograph, finger print or iris scan, against a given Aadhaar number.

158. It is further submitted that such use of the biometric information is an essential function of the Aadhaar Act. The use of biometrics, which is protected by the fundamental right to privacy in physical autonomy. Using biometric information for enrolment and

verification, being the essential feature of the Act, it is submitted that the power to change its scope under Section **2(g)** and **2(j)** and power to determine biometric information required for enrolment cannot be delegated to the UIDAI.

159. Without prejudice to the above, it is submitted that, the Aadhaar Act has not laid down any guidelines for determining the additional biological attribute that may be added to the definition of biological and/or core biological information that may be used for enrolment and/or authentication. The Act also fails to specify any principle or lay down a condition under which a new biological attribute may be added to the definition of biometric or core biometric information. Such delegation is unguided and allows the UIDAI to even make additional biometric information such as voice, ear lobes, and DNA mandatory for enrolment without any guidelines in addition to the already existing biometric information i.e. fingerprints, iris and photograph. Therefore, Section 23(2)(a), Section 2(g) and Section 2(j) are vitiated by *excessive delegation and unguided power*.

160. Further, **Section 6** of the Act provides that the UIDAI "*may require Aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations, so as to ensure continued accuracy of their information in the Central Identities Data Repository*"

161. The main object of the Act of ensuring targeted delivery of subsidies, benefits and services, is essentially met through the statutory provision for enrolment of residents. Therefore, laying down the broad principles related to enrolment, as has been done under Chapter II (Enrolment) of the Act, is an essential feature of the Act. Hence, delegating such power to UIDAI to decide updating demographic or biometric information is not permissible.

162. Without prejudice to the above, it is submitted that in Section 6 under Chapter II, the legislature provides no guidelines under which the Aadhaar number holders may be asked to update demographic and biometric information. Instead the legislature has delegated the power to the UIDAI to define the circumstances under which an update of demographic and biometric information may be sought. This is a clear delegation of the essential legislative power to the executive, which is excessive and without any guidelines.

163. Further, Section **23(2)(g)** read with Section **54(2)(l)** of the Act extends empowers the UIDAI to omit or deactivate an Aadhaar number or information relating thereto, in a manner that may be laid down by the regulations issued by the UIDAI itself.

164. It is submitted that the essential feature of the Act is the entitlement of every resident of India to obtain an Aadhaar number by submitting her demographic and biometric information. Therefore, the power to decide omission or deactivation of an Aadhaar number cannot be delegated. Hence, powers under Sections **23(2)(g**) and Section **54(2)(l)** have been delegated excessively.

165. Without prejudice to the same mentioned above, it is submitted that the Act does not lay down any guidelines for omission or deactivation of Aadhaar number. For instance, the Act does not even provide for hearing to the Aadhaar number holder before the cancellation of the Aadhaar number. The Act also does not provide for circumstances under which an Aadhaar number may be omitted or deactivated. Therefore, powers under Section 23(2)(g) and Section 54(2)(l) are have been delegated to the UIDAI in excess and without any guidelines.

166. Similarly, Section 10 of the Aadhaar Act allows the UIDAI to engage one or more entities to establish and maintain the CIDR to perform any function as may be specified by the Regulations. It is submitted that maintenance of the CIDR is the essential feature of the Act, as the CIDR holds the sensitive identity information of the residents who have enrolled for Aadhaar. Hence, this essential feature cannot be delegated to the UIDAI or further delegated to a third party entity as envisaged by Section 10. Hence, the power under Section 10 has been delegated in excess.

167. Assuming that such power can be delegated to the UIDAI, the Act fails to provide any guidelines or principles for engaging such entities for maintenance of the CIDR. Therefore, the powers delegated to the UIDAI under Section 10 are in excess and without guidelines.

168. In ***Vasantlal Maganbhai Sanjanwala*** v. ***The State of Bombay And Ors.*** 1961 SCR (1) 341, this Hon'ble Court had provided two tests to be subjected to a statute challenged on the ground of excessive delegation. The two tests were:

a. Whether the legislation delegates essential legislative function or power?

b. Whether the legislature has enunciated its policy and principle for the guidance of the delegate?

169. It is further submitted that when the Legislature delegates without laying down any guideline for the executive, it confers an arbitrary power on the executive which could be used to modify the policy without any control over the subordinate legislation. (See ***Devi Das Gopal Krishnan & Ors*** v. ***State Of Punjab & Ors.***, 1967 SCR (3) 557 at para 15).

170. Further, essential legislative functions could be delegated provided the legislative policy is enunciated with sufficient clarity and a standard is laid down. (See ***Ajoy Kumar Banerjee*** v. ***Union of India***, (1984) 3 SCC 127 at para 29)

171. In light of the above, it is submitted that Sections 2(g), 2(j), 6, 23(2)(a), 23(2)(b) and 25(2)(g) delegate excessive powers to the UIDAI without any guidelines.

**a. Several provisions of the Aadhaar Act, 2016 are liable to be struck down for reasons of being vague and overbroad.**

172. The Aadhaar Act was enacted on 26th March 2016 and the regulations were passed by the UIDAI through a notification dated 12th September 2016. Several provisions of the Act and the regulation are liable to be struck down for the reasons of vagueness and over-breath.

173. Section **29(1) (a)** of the Aadhaar Act prohibits the sharing of core biometric information collected or created under the Act. However, Section 29 (4) allows the Aadhaar number and core biometric information to be published, displayed or posted publicly "as may be specified by regulations". While being in direct conflict with Section 29(1)(a), Section 29(4) also gives the Authority an unlimited power and discretion to frame regulations on when and how the Aadhaar number and core biometric information can be publicly displayed.

174. Informational Privacy has been held to be an important facet of right to privacy by this Hon'ble Court (***Justice K.S. Puttaswamy*** v. ***Union of India***, (2017) 10 SCC 1, page 264 point no. 5). It has also been held by this Hon'ble Court that information provided by an individual to a third party carries with it a reasonable expectation that it will be utilised only for the purpose it was provided for (***District Registrar & Collector, Hyderabad*** v. ***Canara Bank***, (2005) 1 SCC 496, p. 523 para 53).

175. Therefore, the power given to the Authority by virtue of Section 29(4) to make regulations enabling publication or posting of biometric and Aadhaar information publicly without any guidelines/limitations is a violation of informational privacy under Article 21 of the Act.

176. Regulation **27(1)(b)(iv)** of the Aadhaar (Enrolment and Update) Regulations states that the Authority has the power to cancel the Aadhaar number in "Any other case requiring cancellation owing to the enrolment appearing fraudulent to the Authority". The Authority also has the power to deactivate an Aadhaar number in any case it deems appropriate (**Regulation 28(1)(f)).** These provisions of cancellation and deactivation of Aadhaar numbers casts a wide net without any guidelines or specificity on the reasons for which an Aadhaar number might be cancelled.

177. Further **Regulation 27 (2**) states "*Upon cancellation, services that are provided by the Authority to the Aadhaar number holder shall be disabled permanently*." This indicates that functions such as authentication and access to benefits through Aadhaar scheme will be stopped. As more and more schemes are being linked to the Aadhaar number, deactivation or cancellation of the Aadhaar number without as much as giving the Aadhaar holder an opportunity to be heard will inevitably lead to denial of benefits to the person. This is a violation of Right to life under Article 21 and Article 14 of the Constitution. No conditions are laid down. From accessing welfare and benefits, it leads to the civil death of a person.

178. In the case of ***K.A. Abbas*** v. ***Union of India*** (1970) 2 SCC 780 at page 799 at para 46), it was held that when a law allows persons applying it to be in a boundless sea of uncertainty and the law prima facie takes away a guaranteed freedom; the law must be

held to offend the Constitution. It was further stated that this invalidity of the law arises from the probability of the misuse of the law to the detriment of the individual.

179. It has been stated by this Hon'ble Court that when expressions are so vague that they are capable of unrestrained abuse, they must be struck down (***A.K. Roy*** v. ***Union of India***, (1982) 1 SCC 271 at page 319 at para 65). More recently in the case of ***Shreya Singhal*** v. ***Union of India***, ((2013) 12 S.C.C. 73 at p.167, para 87), Section 66A of the Information Technology Act was struck down on the grounds of being vague and arbitrary. It was held that "Section 66A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net". It was further held that "not only are the expressions used in Section 66A expressions of inexactitude but they are also over broad and would fall foul of the repeated injunctions of this Court that restrictions on the freedom of speech must be couched in the narrowest possible terms" (p.169, para 90).

180. In the light of the above, the abovementioned provisions of the Act and Regulations grant an over-broad and unlimited discretionary power to the Authority for disclosure of information and deactivation/cancellation of Aadhaar number. The terms used such as "as may be specified by regulations" in respect of public disclosure of Aadhaar number or core biometric information and "any case it deems appropriate" in respect of deactivation of Aadhaar number are extremely vague allows arbitrariness by officers exercising this power. Thus Section 29 (4) of the Aadhaar Act, Regulations 27(1)(b)(iv) and 28(1)(f)) of the Aadhaar (Enrolment and Update) Regulations are liable to be struck down on the grounds of vagueness and over-breadth.

**(B) That Section 33(2) of the Aadhaar Act is Overbroad and Constitutionally Invalid**

181. With regard to **Section 33(2),** the powers granted to the Executive under Section 33(2) are unreasonably wide, given the egregious violation of privacy that would result from the inspection of an Indian resident's Aadhaar authentication records. Section 33(2) permits the absolute disclosure of all demographic information, authentication records and meta data of an Aadhaar holder, and permits the Executive to direct the usage of core biometric information by the UIDAI for any purpose (without actual disclosure of

the underlying core biometric information). There are no safeguards on the use of this power, and no independent review mechanism to ensure that this power is not misused; the Oversight Committee is comprised solely of high ranking members of the Executive.

182. In this context, reference is made to European Union jurisprudence with regard to infringements of the right to privacy under Article 8 (2) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which required that any interference with the aforesaid right had to be made '*in accordance with the law*'. In *Amann* v. *Switzerland*, the European Court of Human Rights ("ECHR") drew attention (in para 50) to its established case law, according to which the phrase *"'in accordance with the law' not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects"*. Further, it stated (in para 56) that "*According to the Court's established case-law, a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct (see the Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, pp. 31-32, § 66). With regard to secret surveillance measures the Court has underlined the importance of that concept in the following terms (ibid., pp. 32-33, §§ 67-68):*

> *"The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention ... The phrase thus implies – and this follows from the object and purpose of Article 8 – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident...*
>
> *... Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."*

*It has also stated that "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and*

*must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."*

183. In this context the ECHR analysed impugned provisions of the Federal Criminal Procedure Act ("FCPA") under Swiss Law, which provided for the surveillance of persons suspected or accused of a crime or major offence (including third parties passing information to such persons), and gave the Police the power to provide an investigation and information service in the interests of the Confederation's internal and external security", including by means of 'surveillance' measures. The ECHR found (in para 58) that the FCPA "*contains no indication as to the persons concerned by such measures, the circumstances in which they may be ordered, the means to be employed or the procedures to be observed. That rule cannot therefore be considered to be sufficiently clear and detailed to afford appropriate protection against interference by the authorities with the applicant's right to respect for his private life and correspondence*."

184. Similarly, (in para 76), the ECHR analysed the Swiss Federal Council's Directives of 16 March 1981 applicable to the Processing of Personal Data in the Federal Administration, and found that "*they set out some general principles, for example that "there must be a legal basis for the processing of personal data" (section 411) or that "personal data may be processed only for very specific purposes" (section 412), but do not contain any appropriate indication as to the scope and conditions of exercise of the power conferred on the Public Prosecutor's Office to gather, record and store information; thus, they do not specify the conditions in which cards may be created, the procedures that have to be followed, the information which may be stored or comments which might be forbidden. Those directives, like the Federal Criminal Procedure Act and the Federal Council's Decree of 29 April 1958 on the Police Service of the Federal Public Prosecutor's Office, cannot therefore be considered sufficiently clear and detailed to guarantee adequate protection against interference by the authorities with the applicant's right to respect for his private life.* (para 77) *The creation of the card on the applicant was not therefore "in accordance with the law" within the meaning of Article 8 of the Convention*."

185. Applying the same reasoning to the Aadhaar Act, Section 33(2) is neither accessible nor foreseeable and does not satisfy the requirement of quality of law that is required to satisfy the principle of 'legality'. It contains no indication of the circumstances in which

the power may be exercised, or the procedures to be observed, and is therefore, neither sufficiently clear nor adequately detailed to afford appropriate protection against interference by the authorities with an Aadhaar holder's right to privacy.

186. In *United States* v. *United States District Court* (407 U.S. 297 (1972)), the United States Supreme Court considered the question of whether the President had the power to authorise electronic surveillance in internal security matters without prior judicial approval. While considering the power of the President and the legitimate need to safeguard domestic security with the use of electronic surveillance, the Court went into the question of whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such surveillance is undertaken; a requirement that was enshrined in the Fourth Amendment. In this context, the Court observed that "*the price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorised official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.*" Further, in the context of the Fourth Amendment and the executive officers of the Government assigned the duty and responsibility to enforce laws, investigate and prosecute, the Court observed that "*those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgement, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech*." Accordingly, the Court held that "*the Fourth Amendment contemplates a prior judicial judgement, not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individuals freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government… The independent check upon the executive discretion is not satisfied, as the Government argues, by "extremely limited" post-surveillance judicial review. Indeed, post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights*."

187. In the aforesaid case, the Government offered several justifications for exempting surveillance ordered in the interests of national security from judicial review, including (i) the contention that the requirement of judicial review would obstruct the President in the discharge of his constitutional duty to protect domestic security, and (ii) the security considerations arising in such matters involved a large number of complex and subtle factors beyond the competence of the courts to evaluate. In response, the Court held that while there was pragmatic force to the Government's position on the need to take swift action in cases involving national security, "*the circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech.* ***Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent****. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case, we hold that this requires an appropriate prior warrant procedure. We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. Certainly courts can recognize that domestic security surveillance involves different considerations from the surveillance of "ordinary crime." If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.*

188. In conclusion, the Court held that "*the Government's concerns do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance. Although some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values. Nor do we think the Government's domestic surveillance powers will be impaired to any significant degree. A prior warrant establishes presumptive validity of the surveillance and will minimize the burden of justification in post-surveillance judicial review. By no means of least importance will be the*

*reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur."* Extending this reasoning to Aadhaar Act, it is evident that the power of granted to the Executive under Section 33(2) is overbroad and constitutionally problematic, particularly since there is no independent oversight of the exercise of this power.

189. This Hon'ble Court in the case of ***People's Union Of Civil Liberties vs Union Of India*** **(1997) 1 SCC 301** (hereinafter PUCL) had noted that Section 5(2) of the Indian Telegraph Act, 1885 allowing phone tapping in the interest of national security, public order, investigation of crime and similar objectives, lacked just and fair procedure for regulating the exercise of power (See para 31).

190. This Hon'ble Court had duly noted in *PUCL* that, "*…in the absence of any provision in the statute, it is not possible to provide for prior judicial scrutiny as a procedural safeguard… …The power to make rules under Section 7 of the Act has been there for over a century but the Central Government has not thought it proper to frame the necessary rules despite severe criticism of the manner in which the power under Section 5(2)has been exercised…In order to rule-out arbitrariness in the exercise of power under Section 5(2) of the Act and till the time the Central Government lays down just, fair and reasonable procedure under Section 7(2)(b) of the Act, it is necessary to lay down procedural safeguards for the exercise of power under Section 5(2) of the Act so that the right to privacy of a person is protected.*" See para 34 of the judgment.

191. Therefore, the guidelines by this Hon'ble Court in *PUCL* were laid down expecting that the Central Government would provide for appropriate procedure in the form of judicial scrutiny. Therefore, where a statute provides for invasion of privacy of an individual, procedural safeguard for exercise of this power would include providing for prior judicial scrutiny.

192. Section 33(2) of the Aadhaar Act allows disclosure of identity information and authentication records pursuant to an order of an officer not below the rank of a Joint Secretary in the interest of "national security". The proviso to Section 33(2) states that the order has to be reviewed by an Oversight Committee consisting of the Cabinet

Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology, before it takes effect. It is submitted that Section 33 (2) provides no guidelines or limitations other than the effective duration of the said order. It is submitted that personal liberty can only be infringed by due process of law provided that the law is just, fair, reasonable and non-arbitrary. (***Maneka Gandhi* v. *Union of India*).** By simply putting a law in place does not suffice, the law has to clearly indicate the scope of such discretion and has to provide for prior judicial scrutiny.

193. Section 33(2) of the Act fails to provide for any safeguards against arbitrary exercise of power by a Joint Secretary, who's a part of the executive. Even the Oversight Committee which shall review the order of the Joint Committee comprises of the members of the executive. Vide Section 33(2) the Act empowers the executive with the power of judicial scrutiny. In absence of any judicial scrutiny, procedure under Section 33(2) allowing disclosure of Aadhaar information is arbitrary. Therefore, Section 33(2) is constitutionally invalid.

### (C) That Section 57 of the Aadhaar Act is Overbroad and Constitutionally Invalid

194. Moreover, the Aadhaar Act does not specifically contemplate or regulate such application of the Aadhaar Project, which is clearly beyond the ambit of the Aadhaar Act, including Section 57. This causes significant problems, particularly when because the India-Stack permits the Aadhaar Project to be used for purposes that it was not intended for and is not appropriate for. For instance, the use of Aadhaar e-KYC as sufficient documentation for opening a bank account is problematic, as Aadhaar demographic data is not verified and therefore could be incorrect. Another example of the problematic usage of Aadhaar is the 'E-Sign', a service that enables someone to use Aadhaar authentication to legally sign and execute an agreement. However, this poses a grave danger of fraud – given that the only two things needed for E-Sign are the Aadhaar number and biometrics of the Aadhaar number holder, both of which are not secret information: the Aadhaar number is revealed to the requesting entities (and has been leaked numerous times), and biometrics are easily recreated / obtained / skimmed.

195. By virtue of the open ended nature of Section 57, private entities are often able to insist and coerce customers into submitting their Aadhaar data, on account of the unequal bargaining power in the market. It is submitted that the Aadhaar Act did not envisage such usage of the Aadhaar technology by private players. The Respondents may claim that Section 57 permits this, but if such a contention were true, then Section 57 would be unconstitutionally over broad, given the violation of privacy that ensues from the unrestricted usage of Aadhaar for such purposes. Reference is made in this context to the following judgements:

(i) ***Shreya Singhal* v. *Union of India*** (2015) 5 SCC 1

[para 87] "*In point of fact, Section 66A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of the Section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total… It is thus clear that not only are the expressions used in Section 66A expressions of inexactitude but they are also over broad and would fall foul of the repeated injunctions of this Court that restrictions on the freedom of speech must be couched in the narrowest possible terms…"*

At para 90 **"…***We, therefore, hold that the Section is unconstitutional also on the ground that it takes within its sweep protected speech and speech that is innocent in nature and is liable therefore to be used in such a way as to have a chilling effect on free speech and would, therefore, have to be struck down on the ground of overbreadth*."

(ii) ***Kartar Singh* v. *State of Punjab*** (1994) 3 SCC 569

[para 130] "*It is the basic principle of legal jurisprudence that an enactment is void for vagueness if its prohibitions are not clearly defined. Vague laws offend several important values. It is insisted or emphasized that laws should give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Such a law impermissibly delegates basic policy matters to policemen and also judges for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. More so uncertain and undefined words deployed inevitably lead citizens to*

*"steer far wider of the unlawful zone ... than if the boundaries of the forbidden areas were clearly marked.*"

196. An example of this is the development of commercial applications by private entities using the underlying Aadhaar technology and the CIDR. This is directly facilitated by the UIDAI, which has developed technology that permits outside entities to access the CIDR in a controlled manner (through the authentication facility). This technology, which is known as the 'India Stack', is a collection of 'Application Programming Interfaces' ("API"), i.e. a set of functions and procedures attached to an operating system or database, which allows the creation of applications in order to access the features or data of that operating system or database (in this case, the CIDR). The India stack permits private entities to build business models utilising the Aadhaar platform, by enabling such entities to to perform Aadhaar authentications, either directly or indirectly, and thereby identify Aadhaar holders for their own private purposes. Numerous private entities have tapped into this facility, and are currently generating vast amounts of revenue and business on the basis of the Aadhaar project. Such private players have a significant vested interest in the Aadhaar project, given that it generates significant profit and personal data for them.

197. The use of private personal information of Indian residents by such entities for various commercial purposes is again violative of the right to privacy, particularly since this is facilitated by State-owned technology.

## VI. The Aadhaar Act renders the Orders of this Hon'ble Court ineffective

198. The Hon'ble Supreme Court of India has at least six times sought to restrain the mandatory of use of Aadhaar and the proliferation of its use.

199. There are several instances before this Hon'ble Court where the orders of the Court have been violated – including Contempt Petitions and IAs. (Contempt Petitions in W.P. (C) 37/2015 and IAs thereto and the I.A. in W.P. (C) 833/2013 are illustrative.

200. A summary of the orders is given below.

| Date | Order |
|---|---|
| 23.09.2013 | In W.P. (Civil) No. 494/2012 and clubbed matters, where the validity of the Unique ID (UID) scheme called "Aadhaar" Scheme has been challenged in numerous petitions, the Hon'ble Supreme Court directed as follows:<br><br>*"In the meanwhile, no person should suffer for not getting Aadhaar Card in spite of the fact that some authority had issued a circular making it mandatory and when any person applies voluntarily, it may be checked whether that person is entitled for it under law and it should not be given any illegal immigrant"* |
| 24.03.2014 | The Hon'ble Supreme Court passed an order in SLP (Crl) No. 2524 of 2014, wherein it was directed as follows:<br><br>*"In the meanwhile, the present petition is restrained from transferring any biometric information of any person who has been allotted the Aadhaar Number to any other agency without his consent in writing. More so, no person shall be deprived of any service for want of Aadhaar Number in case he/she is otherwise eligible/entitled. All the authorities are directed to modify their forms/ circulars/ likes to as to not compulsorily require the Aadhaar Number in order to meet the requirement of the interim order passed by this Court forthwith".* |
| 16.03.2015 | In W.P. (Civil) No. 494/2012 and clubbed matters, the Hon'ble Supreme Court in its order directed as follows:<br><br>*"In the meanwhile, it is brought to our notice that in certain quarters, Aadhaar identification is being insisted upon by the various authorities, we do not propose to go into the specific instances.*<br><br>*Since Union of India is represented by learned Solicitor General and all the States are represented through their respective counsel, we expect that both the Union of India and States and all their functionaries should adhere to the Order passed by this Court on 23rd September, 2013."* |
| 11.08.2015 | The Hon'ble Supreme Court passed the following Interim Order in the above said matters: |

| Date | Order |
|---|---|
| | *"Having considered the matter, we are of the view that the balance of interest would be best served, till the matter is finally decided by a larger Bench if the Union of India or the UIDA proceed in the following manner:-*<br><br>*The Union of India shall give wide publicity in the electronic and print media including radio and television networks that it is not mandatory for a citizen to obtain an Aadhaar card;*<br><br>*The production of an Aadhaar card will not be condition for obtaining any benefits otherwise due to a citizen;*<br><br>*The Unique Identification Number or the Aadhaar card will not be used by the respondents for any purpose other than the PDS Scheme and in particular for the purpose of distribution of foodgrains, etc. and cooking fuel, such as kerosene. The Aadhaar card may also be used for the purpose of the LPG Distribution Scheme;*<br><br>*The information about an individual obtained by the Unique Identification Authority of India while issuing an Aadhaar card shall not be used for any other purpose, save as above, except as may be directed by a Court for the purpose of criminal investigation."* |
| 15.10.2015 | The Order dated 11.08.2015. The Constitution Bench directed as follows:<br><br>*"3. After hearing the learned Attorney General for India and other learned senior counsels, we are of the view that in paragraph 3 of the Order dated 11.08.2015, if we add, apart from the other two Schemes, namely, P.D.S. Scheme and the L.P.G. Distribution Scheme, the Schemes like The Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), National Social Assistance Programme (Old Age Pensions, Widow Pensions, Disability Pensions) Prime Minister's Jan Dhan Yojana (PMJDY) and Employees' Provident Fund Organisation (EPFO) for the present, it would not dilute earlier order passed by this Court. Therefore, we now include the aforesaid Schemes apart from the other two Schemes that this Court* |

| Date | Order |
|---|---|
| | *has permitted in its earlier order dated 11.08.2015.*<br><br>*We impress upon the Union of India that it shall strictly follow all the earlier orders passed by this Court commencing from 23.09.2013.*<br><br>*We will also make it clear that the Aadhaar card Scheme is purely voluntary and it cannot be made mandatory till the matter is finally decided by this Court one way or the other."* |
| 14.09.2016 | A challenge was made in W. P. (Civil) No. 686/2016 before the Hon'ble Supreme Court where Aadhaar was made mandatory for various education schemes, wherein it was directed as follows:<br><br>*"Having regard to the facts and circumstances of the case, the material evidence available on record and the submissions made by learned senior counsel we stay the operation and implementation of letters dated 14.07.2006 (i.e. Annexure P-5, P-6 and P-7) for Pre-Matric Scholarship Scheme, Post-Matric Scholarship Scheme and Merit-cum-Means Scholarship Scheme to the extent they have made submission of Aadhaar mandatory and direct the Ministry of Electronics and Information Technology, Government of India i.e. Respondent No.2 to remove Aadhaar number as a mandatory condition for student Registration form at the National Scholarship Portal of Ministry of Electronics and Information Technology, Government of India at the website http://scholarships.gov.in/newStudentRegFrm and stay the implementation of clause (c) of the 'Important Instructions' of the advertisement dated 20.08.2016 for the Pre-Matric Scholarship Scheme, Post-Matric Scholarship Scheme and Merit-cum-Means Scholarship Scheme, during the pendency of this writ petition."* |

201. It is submitted that even though the Aadhaar Act has been passed, it cannot form the basis for allowing issuance of notifications requiring mandatory Aadhaar for seeking benefits. One such instance is the notification of the Ministry of Health and Family Welfare dated 16.06.2017 that allows access to Tuberculosis treatment under the Revised National Tuberculosis Control Programme, subject to the production of Aadhaar number or proof of Aadhaar enrolment.

202. Such notifications provisions are in clear violation of the interim orders of this Hon'ble Court wherein it had stated that, "In the meanwhile, no person should suffer for not getting Aadhaar Card in spite of the fact that some authority had issued a circular making it mandatory". Hence, any notification requiring compulsory production of Aadhaar would be contrary to the orders of this Hon'ble Court. It is submitted that even if the enactment of the Aadhaar Act allows the States and/or Executive agencies to mandate Aadhaar for identification, such power may be exercised only after this Hon'ble Court vacates the above mentioned orders.

203. It is a well settled principle in law that, "*when once an order has been passed which the Court has jurisdiction to pass, it is the duty of all persons bound by it to obey the order so long as it stands, and it would tend to the subversion of, orderly administration and civil Government, if parties could disobey orders with impunity*." (*The State of Bihar* v. *Rani Sonabati Kumari* 1961 SCR (1) 728 at para 34).

204. Therefore, the notifications mandating the use of Aadhaar number for identification is an impermissible executive exercise and should be set aside.

## VII. Conclusion

205. In conclusion, it is reiterated that the Aadhaar Project represents an unjustifiable violation of the right to privacy and right to life of Indian residents.

206. The Aadhaar Project was not backed by a legislation for the majority of the time of its existence, when grave violations of privacy and the right to life occurred. Further, the existing Aadhaar Act does little to prevent continuing and repeated violations of Article 14 and 21.

207. The Aadhaar Project is bereft of a legitimate State aim. This is because the stated aim, which finds place in the Aadhaar Act, is not the underlying objective that is being

pursued by the Aadhaar project. Indeed, the Aadhaar Project serves a plethora of unauthorised objectives, while continuing to fail the stated aim in the legislation – which is the effective targeting beneficiaries of government welfare schemes. The enrolment process of the Aadhaar project does not involve any verification of even the demographic information submitted, let alone the eligibility of an individual for a scheme.

208. Moreover, ***the State has misrepresented the cause of leakages in its welfare programs***, by stating that such leakages are caused by ghosts and duplicate beneficiaries. It is submitted that there is little evidence to show that such losses in State-funded welfare schemes are on account of such duplicates and fakes and ghosts; in this regard, attention is drawn to the responses of the Punjab Government and the Indian Oil Corporation Limited to RTI applications seeking information on duplicates or fakes discovered in the PDS system and LPG connections respectively. Responses in the case of both RTI applications stated that no documents were available that indicated the existence of such fakes and duplicates, which indicates that no proper diligence was done of the problem that was sought to be fixed, thereby impugning the stated aim of the Aadhaar Act itself. See **Annexure 12** and **13, running pages 144-146 of the Petitioner's Vol II**, for the RTI Application dated 03.03.2014 and corresponding response from Food Civil Supplies and Consumer Affairs Department, Punjab Government, and see **Annexure 14, 15 and 16, running pages 147-150 of the Petitioner's Vol II**, for the RTI Application dated 10.10.2013 and corresponding responses from Indian Oil Corporation Limited.

209. Instead the main objectives that are actually being serviced by the Aadhaar Project are those pertaining to commercial interests, profiling and State surveillance. Further, the Aadhaar Project lacks basic security and technical safeguards to ensure the safety of sensitive personal information of Aadhaar holders; moreover, the safety of the data collected by the UIDAI has already been compromised through numerous instances of breaches, hacking, theft and (both intentional and inadvertent) public disclosure.

210. The Aadhaar system also devalues the notion of the social contract between the State and its residents. This is because the very concept of the identity of an individual has been subjected to a probabilistic process which:

(i) remains unproven in the Indian context;

(ii) is entirely probabilistic and therefore uncertain; and

(iii) is under the control of the State and independent of the individual.

Accordingly, by subjecting a person's identity to the uncertainty and probabilities of a technical process that remains unproven in the Indian context, the Aadhaar Project has made identity itself uncertain. If the identity of an Indian resident is not confirmed by the Aadhaar system, then that resident's identity is nullified and very existence – in the eyes of the State – ceases. Effectively, the State has established means by which it can void the social contract (i.e. the Constitution of India) with its residents.

211. In his magnum opus, 'The Social Contract' (1762), Rousseau contends that the only legitimate political authority is an authority that has been consented to by all people, their consent forming the basis of the social contract between that authority and the people. His central hypothesis is that a government gains its legitimacy and right to govern from the continuing consent of the people. Therefore, the very idea of subjecting people to an uncertain process that can vitiate their 'consent' and effectively their 'right to life' within the sovereign, is unacceptable; this amounts to a fundamental alteration of the terms of the social contract between citizen, residents and State, and an monumental shift of power. Moreover, the Aadhaar lacks legitimate and informed consent, particularly for the enlarged scope to which it has now been expanded. An Indian resident is nothing – a ghost or an alien – if a small biometric scanner connected to a porous database says that he is not who he was born as.

212. For these reasons, it is submitted that the Aadhaar Project is *ultra vires* the Constitution of India, and that it must be abandoned, with proof of destruction of Aadhaar data provided to this Court.

## AADHAAR ACT v. AADHAAR PROJECT


Excessive Data Collection during Enrolment (KYR+)

Remote Seeding of Parallel Databases with Aadhaar data

Unauthorised Access to CIDR for numerous entities

State Resident Data Hubs

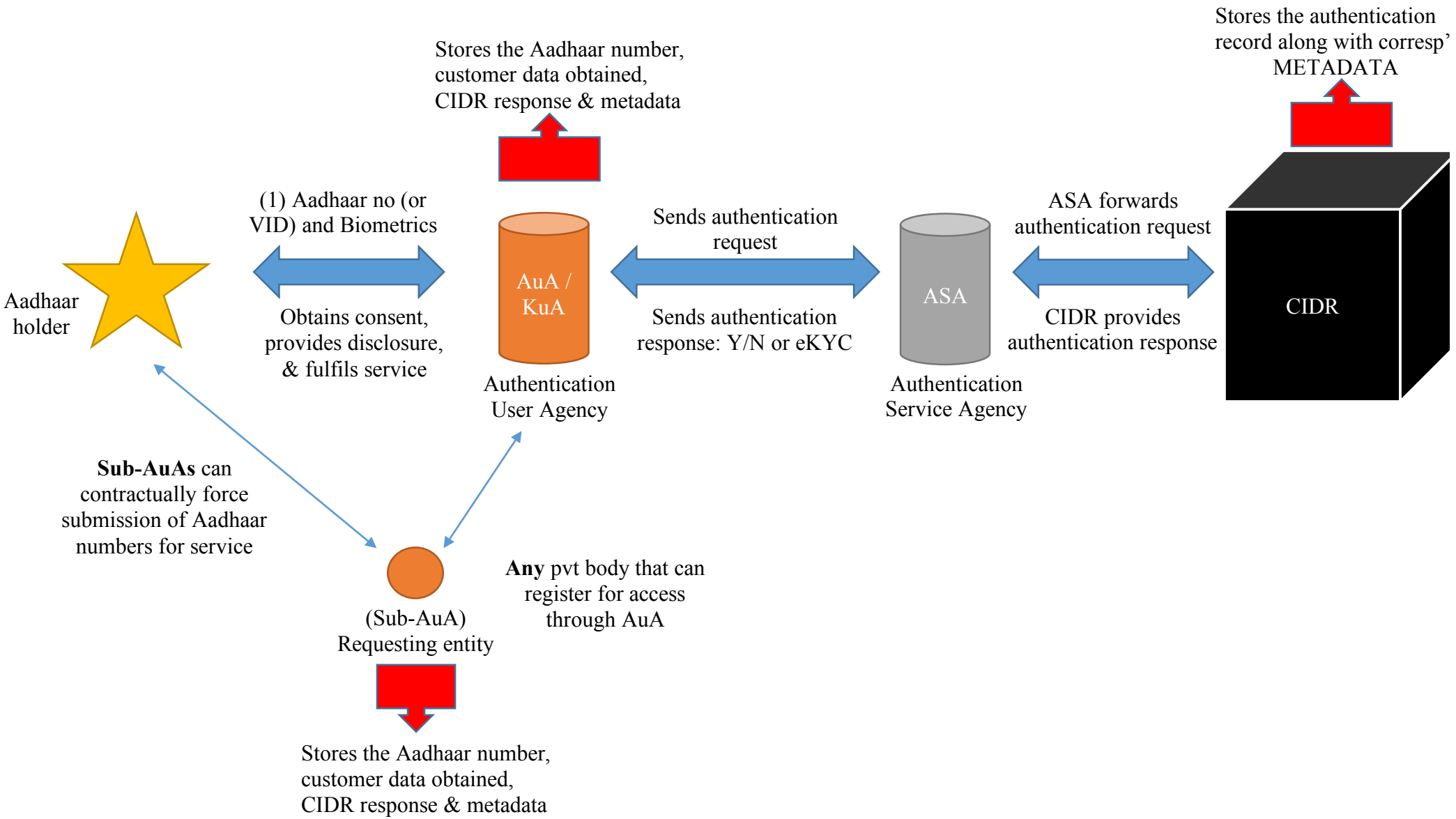
Private Usage of the Aadhaar Technology

Illegal Aggregation of Data within CIDR

Unregulated Power of Surveillance and Profiling by State

**UNREGULATED BY THE AADHAAR FRAMEWORK**

# AADHAAR AUTHENTICATION PROCESS



**The Data Trail of Aadhaar Usage**