IN THE SUPREME COURT OF INDIA

CIVIL WRIT JURISDICTION

WRIT PETITION (c) NO.494 of 2012 & Connected Cases

Justice (Retd) KS Puttaswamy and Anr ...Petitioners

v.

Union of India and others ...Respondents

A. RESPONSE TO THE LEGAL QUERIES RAISED BY PETITIONERS IN WP (CIVIL NO. 1056 OF 2017) NACHIKET UDUPA AND ANOTHER VERSUS UNION OF INDIA

1. **What are the figures for authentication failures, both at the national and state level? Please also provide a breakup, between fingerprints and iris?**

   Answer: UIDAI cannot provide authentication failure rates at the state level since it does not track the location of the authentication transactions. Authentication failure rate at national level is as below:

MODALITY	UNIQUE UID PARTICIPATED	FAILED UNIQUE UID	FAILED %
IRIS	10850391	927132	8.54%
FINGER	616363346	36962619	6.00%

   It must be stated that authentication failures do not mean exclusion or denial from subsidies, benefits or services since the Requesting Entities are obliged under the law to provide for exception handling mechanisms.

2. **In case a person who is claiming a biometric exception (e.g. because she is a leprosy patient) does not have a mobile phone number, or has not given it in the enrolment form, or if the phone number changes-How will her Aadhaar enrolment and subsequent authentication occur? Under which provision of law?{Refer Slide 6}**

Answer:

- Aadhaar enrolment is done for all residents, even of residents with Leprosy. Biometric exception process is defined in the UIDAI resident enrolment process.
- In the case of a leprosy patients, who may not be able to do fingerprint authentication, iris authentication can be used for update (and add the mobile number). This was the reason for multi modal enrolment and authentication being selected for use in Aadhaar.
- Only in an unlikely scenario where BOTH iris and fingerprint cannot be used for authentication, the mobile number is one of the methods for authentication. In cases where authentication through mobile number is not possible or feasible, the requesting entities have to provide their own exception and backup mechanism to ensure services to Aadhaar holders. As part of the exception handling mechanism, UIDAI has already implemented a digitally signed QR code into eAadhaar which allows agencies to verify the Aadhaar card in an offline manner and trust the data (based on digital signature validation) without accessing eKYC API service of UIDAI.[1]
- The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016 (Section 5) And Aadhaar (Enrolment And Update) Regualtions, 2016 (Regulation 6) defines special provision for enrolment of residents with biometric exception.
- Further, as per Regulation 14(i) of Aadhaar (Authentication) Regulations, 2016, "*requesting entity shall implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication services to Aadhaar number holders*".
- Accordingly, DBT Mission Cabinet Secretariat has issued a detailed circular dated 19.12.2017 regarding exception handling during use of Aadhaar in Benefit Schemes of Government.

[1] Note that this is a simple offline mechanism to quickly verify the legitimacy of the Aadhaar card. But, it does not ensure the person holding the card is the owner of that Aadhaar number. It needs either manual check of photo against the face of the individual (like the way ID is verified at the entry of airports for example) or some form of electronic authentication using Aadhaar authentication API or agency specific authentication scheme. QR code based verification allows Aadhaar number holders to use their ID on a day to day purpose without using online eKYC authentication. The verification through offline QR code can be used for those purposes or use cases where proof of presence or proof of ownership of card is not required.

3. **Are there any surprise checks, field studies done to check the authenticity of the exemption registers?**

Answer: As per Regulation 14(i) of Aadhaar (Authentication) Regulations, 2016, "*requesting entities shall implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication services to Aadhaar number holders*". Therefore, this exception handling mechanism is to be implemented and monitored by the requesting entities and in case of the government, their respective ministries. Further, DBT Mission Cabinet Secretariat had issued a detailed circular dated 19.12.2017 on exception handling and audit of exceptions.

4. **Between the ages of 5-15 years, can a school, as an "introducer", enrol a child without parental consent?{Refer Slides 9 and 10}**

Answer: School officials, if permitted to act as 'introducer' can enrol only when there is a parental consent to enrol. The disclosure requirement as per section 3(2) of The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016 and Aadhaar (Enrolment And Update) Regulations, 2016 (Schedule I) is implemented through the enrolment form which is signed by resident making it informed disclosure. In case of children, the consent form will be signed by the parent/guardian.

5. **Once a child attains the age of 18 years is there any way for them to opt out or revoke consent ?{refer Slide 9 and 10}**

Answer:

No. It is not permissible under Aadhaar Act, 2016. However, residents have the option of permanently locking their biometrics and only temporarily unlock it when needed for biometric authentication as per Regulation 11 of the Aadhaar (Authentication) Regulations, 2016.

6. **What is the status of the enrolments done by the 49,000 blacklisted enrolment operators? Please provide the number of enrolments done by them?**

Answer : UIDAI has a policy to enforce the process guidelines and data quality check during the enrolment process. 100% of the enrolment done by operators

undergoes a quality assurance check, wherein every enrolment passes through a human eye. Any Aadhaar enrolment found to be contrary to the UIDAI process, the enrolment itself gets rejected and Aadhaar is not generated. The resident is advised to re-enroll.

Once an operator is blacklisted or suspended, further enrolments cannot be carried out by him during the time the order of blacklisting/suspension is valid.

7. **What are the total numbers of biometric de-duplication rejections that have taken place till date? In case an enrolment is rejected either for (a) duplicate enrolment and (b) other technical reason under Regulation 14 of the Aadhaar (Enrolment and Update) Regulations, what happens to the data packet that contains the stored biometric and demographic information?**

Answer :

The total number of biometric de-duplication rejections that have taken place are 6.91 cr. as on 21st March 2018. These figures do not pertain to the number of unique individuals who have been denied Aadhaar enrolment resulting in no Aadhaar issued to them. This figure merely pertains to the number of applications which have been identified by the Aadhaar de-duplication system as having matching biometrics to an existing Aadhaar number holder. The biometric de-duplication system is designed to identify as duplicate those cases where any one of the biometrics (ten fingers and two irises) match. However, very often it is found that all the biometrics match. It is highly improbable for the biometrics to match unless the same person has applied again. There are a number of reasons why the same person might apply more than once. For instance, many individuals innocently apply for enrolment multiple times because of the delay in getting their Aadhaar cards due to postal delays, loss or destruction of their cards or confusion about how the system works. Each time one applies for Aadhaar, the system identifies this as a new enrolment but when it recognises that the individual's biometrics match with already those in the database and thereafter, further checks including manual check through experienced personnels are done. After these exercise if it is found that the person is already registered in the system, it rejects the enrolment application. One of the other main reasons for rejection is that multiple people would put their biometric details like fingerprints for Aadhaar generation either as a fraudulent exercise or by mistake, which also would get

rejected . Since there were many fakes and frauds in the earlier systems, and several reports have found that almost 50% of the subsidies were getting pilfered away by fakes and duplicates in the system, then there would also be several such people who may have tried to defraud the Aadhaar enrolment system as well but failed get multiple Aadhaar numbers due to the stringent Aadhaar de-duplication process. Thus, the mere fact that 6.23 Crore enrolments have been rejected as biometric duplicates does not mean that 6.23 Crore people have been denied an Aadhaar number as has been alleged by the petitioners. Any genuine person who does not have an Aadhaar number and whose enrolment has been rejected can always apply again for enrolment. It is worth noting that none of the de-duplication rejects have come forward to lodge complaints either with the Authority or with the Government about denial of Aadhaar number. None of them have even approached any Court of law. Evidently, the genuine residents have got themselves re-enrolled and the rest are those who were trying to overreach the Aadhaar system by fraudulent means. That explains why no one has approached a court of law complaining denial of Aadhaar number.

All the enrolment packets received by UIDAI (accepted/rejected) are archived in the CIDR irrespective of its status.

8. **If the figure of rejection of enrolment packets was 8 crore, as on 2015 (see parawise reply filed by the Union of India to para (lxxxvi) of Mathew Thomas vs UOI , W.P.(C) No. 37/2015 @pg 71), what is the total rejection figure for enrolment packets as on date? How many field studies/physical verification have been done to ensure that these persons (who have been rejected) are indeed "False or duplicate" enrolments?**

Answer:

- The total rejection figure for enrolment packets is 18.0 cr. as on 26th March, 2018. These rejections are due to various technical reasons like 1. Data quality reject such as address incomplete, name incomplete, use of expletives in names, address etc. photo is of object, photo of photo, age photo mismatch etc 2. OSI validation reject such as operator/supervisor/introducer validation failed,

operator/supervisor/introducer/Head of Family biometric validation failed etc.

- Those whose enrolments have been rejected for any reason and who do not have Aadhaar can re-enrol and obtain Aadhaar. Rejection of enrolments do not mean that the person will never be able to get Aadhaar.

9. **What does "any other appropriate response" under sec. 8(4) of the Aadhaar Act include?**

Answer: "Any other appropriate responses" includes e-KYC or limited e-KYC data. As per Regulation 3 of Aadhaar (Authentication) Regulations, 2016, UIDAI provides two types of authentication facilities, namely—

(i) Yes/No authentication facility; and

(ii) e-KYC authentication facility.

In Yes/No authentication, UIDAI provides the response as Yes or No along with relevant error codes, if any.

In e-KYC authentication, UIDAI provides the demographic data along with photograph and in case of mismatch/error, the relevant error codes.

B. RESPONSE TO THE LEGAL QUERIES RAISED BY PETITIONERS IN WP (CIVIL NO. 829 OF 2013) S G VOMBATKERE & ANR. VS. UNION OF INDIA

1. **Please confirm that no UIDAI official verifies the correctness of documents offered at the stage of enrolment/updating.**

Answer: As per UIDAI process, the verification of the documents is entrusted to the Registrar. For Verification based on Documents, the verifier present at the Enrolment Centre will verify the documents. Registrars/Enrolment agency must appoint personnel for the verification of documents.

2. **Please confirm that UIDAI does not know whether the documents shown at the time of enrolment/updating are genuine or false.**

Answer: The answer is same as in (1) above.

3. **Please confirm:**

(a) **UIDAI does not identify the persons it only matches the biometric information received at the time of authentication with its records and provides a yes/no response;**

Answer : Biometric authentication of an Aadhaar number holder is always performed as 1:1 biometric match against his/her Aadhaar number (identity) in CIDR. Based on the match, UIDAI provides yes or no response. A "yes" response means a positive indeifitcation of the Aadhaar number holder.

Each enrollment is biometrically de-duplicated against all (1.2 billion) residents to issue the Aadhaar number (or Unique Identity).

(b) **UIDAI takes no responsibility with respect to the correctness of the name, date of birth or address of the person enrolled.**

Answer:

The Name/Address/DOB are derived from the POI/POA documents submitted during enrolments.

The enrolment/update packet (encrypted) retains a scanned copy of the POI/POA documents used for the enrolment which can be reviewed in case of dispute.

UIDAI maintains the update history of each Aadhaar number related to changes in Name, Address, Date of Birth etc.

4. **Please confirm:**

(a) **UIDAI takes no responsibility with respect to the correct identification of a person.**

Answer: Please refer to Answer (1) above. Additionally, it may be stated that enrolment of Aadhaar is done through a resident enrolment process and verification of the POI/POA document is done against the acceptable documents, as per the UIDAI valid list of documents as provided in Schedule II and III AADHAAR (ENROLMENT AND UPDATE) REGULATIONS, 2016 read with Regulation 10.

UIDAI takes responsibility in creating and implementing standards, ensuring matching systems installed in CIDR work as they are designed to do, and providing options to Aadhaar holders in terms of controlling their identity (such as updating their data, locking their biometrics, etc.) and accessing their own authentication records.

One of the key goals of Aadhaar is to issue a unique identity for the residents of India. Hence, each enrollment is biometrically de-duplicated against all (1.2 billion) residents to issue the Aadhaar number (or Unique Identity).

Section 4 of Aadhaar lays down the Properties of an Aadhaar No. wherein Section 4(3) reads as "(3) An Aadhaar number, in physical or electronic form **subject to authentication and other conditions**, as may be specified by regulations, may be accepted as proof of identity of the Aadhaar number holder for any purpose."

The requesting entities are at liberty to use any or multiple of authentication mode available under Regulation 4 of Aadhaar (Authentication) Regulations, 2016 as per their requirements and needs of security etc.

(b) **The biometric authentication is based on a probabilistic match of the biometric captured during authentication and the record stored with the CIDR.**

Answer:

Biometric authentication is based on 1:1 matching and therefore in that sense it is not probabilistic. If biometrics are captured well it will lead to successful authentication. If biometrics are not well captured during authentication or an impostor tries authentication, it will lead to authentication failure. Aadhaar Proof of Concept studies show that a vast majority of residents (> 98%) can successfully authenticate using biometric modalities such fingerprints and/or iris.

However, the Aadhaar Act and Regulation provides that an Aadhaar number holder cannot be denied service due to the failure of Aadhaar authentication.

Hence all Aadhaar applications must implement exception processes. Possible methods to implement the exception process include:

- **Family Based Authentication:** Family based applications such as PDS or Health applications may allow authentication by family members to allow resident to avail services

- **Alternate Modalities:** Some applications may use different modalities for exception handling. Alternate modalities include:
    - Iris Authentication
    - OTP Authentication (if allowed by policy)

- **Biometric Fusion:** UIDAI is introducing face authentication as secondary authentication factor to reduce the rate of authentication failures, especially for senior citizens. At this time, face authentication will be used only conjunction with another authentication factor such as finger/iris/OTP.
    - Face + Finger Fusion
    - Face + Iris Fusion
    - Face + OTP Fusion
- **Non Aadhaar Based Exception process:** Applications may implement non-Aadhaar based exception process to ensure that no resident is denied service. Applications need to monitor the use of exceptions in their applications to prevent misuse of the exception process.
- Accordingly, DBT Mission Cabinet Secretariat had issued a detailed circular dated 19.12.2017 regarding Use of Aadhaar in Benefit Schemes of Government - Exception handling.

5. **Please confirm that with respect to individuals under 15 years and over 60 years of age, biometric authentication is likely to fail due to changes in/ fading of biometrics such as finger prints.**

   Answer: Though there is no conclusive evidence to say that biometric authentication success is dependent upon age, slightly higher authentication failure rates have been observed only for fingerprints for senior citizens above the age of 70. A number of exception processes are provided *in answer to Q4b* to prevent denial of service for failure of authentication. Further, in case of any issue in biometric authentication, an Aadhaar number holder may update his/her biometric at any of the Aadhaar enrolment center, which is also provided for in the Aadhaar Act.

6. **Please confirm that the reasons why over 49000 enrolment operators were blacklisted include (a) failure to verify documents presented (b) failure to maintain records of documents submitted (c) misuse of information submitted (d) aiding or abetting false enrolments?**

Answer: UIDAI has a policy to enforce the process guidelines and data quality check during the enrolment process. 100% of the enrolment done by operators undergoes a quality assurance check,. Any Aadhaar enrolment found to be not as per the UIDAI process, the enrolment itself gets rejected and Aadhaar is not generated.

If such mistake by an operator crosses a threshold defined in the policy, the operator is blacklisted/ removed from the UIDAI ecosystem. As such 49,000 operators who have been blacklisted/removed from the UIDAI ecosystem, all the enrolments which were in violation of the process were rejected in the QA stage.

Enrolment operators may be blacklisted for the following reasons:

- Illegally charging the resident for Aadhaar enrollment
- Poor demographic data quality
- Invalid biometric exceptions
- Other process malpratice

7. **Please confirm:**

   (a) At the stage of enrolment, there is no verification as to whether a person is an illegal immigrant.

   (b) At the stage of enrolment, there is no verification about a person being residents in India for 182 days or more in the past 12 months.

   (c) Foreign nationals may enrol and are issued Aadhaar numbers.

   (d) Persons retain their Aadhaar number even after they cease to be resident. This is true of foreign nationals as well.

   Answer:

   (a)At the time of enrolment, verification is done based upon documents provided by the resident. In case any violation of prescribed guidelines comes to light, the concerned Aadhaar is omitted / deactivated.

   (b)This has been included through the Enrolment form where resident undertakes and signs the disclosure.

   "Disclosure under section 3(2) of The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016

   I confirm that I have been residing in India for at least 182 days in the preceding 12 months & information (including biometrics) provided by me to the UIDAI is my own and is true, correct and accurate. I am aware that my information

including biometrics will be used for generation of Aadhaar and authentication. I understand that my identity information (except core biometric) may be provided to an agency only with my consent during authentication or as per the provisions of the Aadhaar Act. I have a right to access my identity information (except core biometrics) following the procedure laid down by UIDAI."

(c) Aadhaar is issued to the resident of India, the resident is defined in Section 2 (v) Under Aadhaar Act, 2016. Aadhaar numbers may be issued to foreign nationals who are resident in India.

(v) "resident" means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment;

A foreign national fulfilling the above criteria is eligible for Aadhaar, provided he submits the acceptable POI/POA document as per the UIDAI valid list of documents.

(d) As per Aadhaar Act 2016, an Aadhaar number is issued to a resident who has been residing in India for at least 182 days in the preceding 12 months.

An Aadhaar number is issued to an individual for life and may be omitted / deactivated in case of violation of prescribed guidelines only. Ineligibility of a person to retain an Aadhaar number owing to becoming non-resident may be treated as a ground for deactivation of Aadhaar number under Regulation 28(1)(f) of the Aadhaar (Enrolment and Update) Regulations, 2016. This is in keeping with Section 31(1) and (3) of the Aadhaar Act, 2016 wherein it is an obligation on an Aadhaar number holder to inform the UIDAI of changes in demographic information and for the Authority to make the necessary alteration.

8. **Please confirm that points of service (POS) biometric readers are capable of storing biometric information.**

Answer: UIDAI has mandated use of Registered Devices (RD) for all authentication requests. With Registered Devices biometric data is signed within the device / RD service using the provider key to ensure it is indeed captured live. The device provider RD Service encrypts the PID block before returning to the host application. This RD Service encapsulates the biometric capture, signing and encryption of biometrics all within it. Therefore, introduction of RD in Aadhaar

authentication system rules out any possibility of use of stored biometric and replay of biometrics captured from other source.

Requesting entities are not legally allowed to store biometrics captured for Aadhaar authentication under Regulation 17(1)(a) of Aadhaar (Authentication)Regulations 2016.

9. **Referring to slide/page 13, please confirm that the architecture under the Aadhaar Act includes (i) authentication user agencies (e.g. Kerala Diary Farmers Welfare Fund Board); (ii) authentication service agencies (e.g. Airtel) and (iii) CIDR (Central Identities Data Repository).**
Answer: UIDAI appoints Requesting Entities (AUA/KUA) and Authentication Service Agency (ASA) as per Regulation 12 of Aadhaar (Authentication) Regulations, 2016. List of Requesting Entities (AUA/KUA) and Authentication Service Agency appointed by UIDAI is available on UIDAI's website. An AUA/KUA can do authentication on behalf of other entities under Regulation 15 and Regulation 16 of Aadhaar(Authentication)Regulations 2016.

10. **Please confirm that one or more entities in the Aadhaar architecture described in the previous paragraph, record the date and time of the authentication, the client IP, the device ID and purpose of authentication.**
Answer: UIDAI does not ask requesting entities to maintain any logs related to IP address of the device, GPS coordinates of the device and purpose of authentication. However, AUAs like banks, telecom etc. in order to ensure that their systems are secure, frauds are managed, they may store additional information as per their requirement under their respective laws to secure their system. Section 32(3) of the Aadhaar Act, 2016 specifically prevents the UIDAI from either by itself or through any entity under its control, keep or maintain any information abou the purpose of authentication.

Requesting entities are mandated to maintain following logs as per **Regulation 18 of Aadhaar (Authentication) Regulations, 2016:**
(a) the Aadhaar number against which authentication is sought;
(b) specified parameters of authentication request submitted;

(c) specified parameters received as authentication response;

(d) the record of disclosure of information to the Aadhaar number holder at the time of authentication; and

(e) record of consent of the Aadhaar number holder for authentication,but shall not, in any event, retain the PID information.

Further, even if a requesting entity captures any other data as per their own requirement, UIDAI will only audit the authentication logs maintained by the requesting entity as per the **Regulation 18(1) of the Aadhaar (Authentication) Regulations, 2016.**

ASAs are not permitted to maintain any logs related to IP address of the device, GPS coordinates of the device etc. ASAs are mandated to maintain logs as per **Regulation 20 of Aadhaar (Authentication) Regulations, 2016.**

(a) identity of the requesting entity;

(b) parameters of authentication request submitted; and

(c) parameters received as authentication response:

Provided that no Aadhaar number, PID information, device identity related data and e-KYC response data, where applicable shall be retained.

11. **Referring to slide /page 7 and 14, please confirm that "traceability" features enable UIDAI to track the specific device and its location from where each and every authentication takes place.**

Answer : UIDAI gets the AUA code, ASA code, unique device code, registered device code used for authentication. UIDAI does not get any information related to the IP address or the GPS location from where authentication is performed as these parameters are not the part of authentication (v2.0) and e-KYC (v2.1) API UIDAI would only know from which device the authentication has happened, through which AUA/ASA etc. This is what the slides meant by traceability. UIDAI does not receive any information about at what location the authentication device is deployed, its IP address and its operator and the purpose of authentication. Further, the UIDAI or any entity under its control is statutorily barred from collecting, keeping or maintaining any information about the purpose of authentication under Section 32(3) of the Aadhaar Act.