

IN THE HIGH COURT OF DELHI AT NEW DELHI
EXTRAORDINARY ORIGINAL CIVIL JURISDICTION

WRIT PETITION (C) NO.5405 OF 2018

IN THE MATTER OF:

SHAMNAD BASHEER

...PETITIONER

VERSUS

UNIQUE IDENTIFICATION

AUTHORITY OF INDIA & ORS.

...RESPONDENTS

INDEX

<u>SL.NO.</u>	<u>PARTICULARS</u>	<u>PAGE NO.</u>
1.	Counter Affidavit on behalf of Respondent No. 1	1-134
2.	<u>ANNEXURE R-1</u> True Copy of the Relevant extracts of the Additional Affidavit in W.P(C) No. 797 of 2016 dated 15.01.2018.	135-144
3.	<u>ANNEXURE R-2</u> True Copy of the Relevant extracts of the Application seeking permission to place certain Additional Documents on Record in W.P (C) No. 1056 of 2017 dated 12.01.2018.	145-156
4.	<u>ANNEXURE R-3</u> True Copy of the Relevant extracts of the Written Submissions on behalf of Mr. K.V. Viswanathan, Sr. Adv. In Writ Petition (C) No. 494/2012.	157-161
5.	<u>ANNEXURE R-4</u> True Copy of the Relevant extracts of the Compilation on behalf of Mr. K.V. Viswanathan, Sr. Adv., Vol. IV-	162-183

	'Centralised Data Storage, Breach and Access', in Writ Petition (C) No. 494/2012.	
6.	<u>ANNEXURE R-5</u> True Copy of the Relevant extracts of the Written Submissions on behalf of Ms. Meenakshi Arora, Sr. Adv. In Writ Petition (C) No. 494/2012.	184-190
7.	<u>ANNEXURE R-6</u> True Copy of the Relevant extracts of the Written Submissions on behalf of Mr. Anand Grover, Sr. Adv. In Writ Petition (C) No. 494/2012.	191-204
8.	<u>ANNEXURE R-7</u> True Copy of the Additional Affidavit dated 09.03.2018 filed before the Hon'ble Supreme Court.	205 - 310
9.	<u>ANNEXURE R-8</u> True Copy of the Order dated 04.02.2019 of Hon'ble Supreme Court.	311-312
10.	<u>ANNEXURE R-9</u> True Copy of the Decision of the Government dated 29.09.2017.	313-315
11.	<u>ANNEXURE R-10</u> True Copy of the notification dated 11.12.2015 issued by Ministry of Communication & Information Technology.	316-317
12.	<u>ANNEXURE R-11</u> True Copy of the Report of the committee On The Outcome Review of the UID Scheme.	318-342
13.	<u>ANNEXURE R-12</u> True Copy of the qualifications, background and experience of the renowned experts in the Security Review Committee.	343-367
14.	<u>ANNEXURE R-13</u> True Copy of the OM Dated 25.3.2017 and D.O. dated 25.03.2017	368
15.	Proof of Service	369
16.	Vakalatnama	370

Filed by:

New Delhi

Dated: ____/____/2019

(Zoheb Hossain)

Counsel for Respondent No.1
S-74, LGF, Greater Kailash Part 1,
New Delhi – 110 048
M. 9999711099

/

IN THE HIGH COURT OF DELHI AT NEW DELHI
EXTRAORDINARY ORIGINAL CIVIL JURISDICTION

WRIT PETITION (C) NO.5405 OF 2018

IN THE MATTER OF:

SHAMNAD BASHEER

...PETITIONER

VERSUS

UNIQUE IDENTIFICATION

AUTHORITY OF INDIA & ORS.

...RESPONDENTS

COUNTER AFFIDAVIT ON BEHALF OF THE RESPONDENT NO. 1

I, Ramesh Kumar S/o Dharm Singh aged about 54 years currently holding the position of Deputy Director, Unique Identification Authority of India, Regional Office, UIDAI, Pragati Maidan, New Delhi – 110 001, do hereby solemnly affirm and state as under:

1. That I am authorized by Respondent No. 1 to file this Affidavit in the present matter and I am well conversant with the facts and circumstances of the present case and am competent to swear the present affidavit on behalf of Respondent No. 1.
2. That I have perused the copy of the above captioned petition and have fully understood the contents thereof. At the outset, I deny all the averments, submissions, statements and allegations made therein

except those that are specifically admitted hereinafter to be true and correct. The contents of the present writ petition to the extent they are inconsistent with the submissions made hereinafter in this affidavit are incorrect and are denied. Unless any averment or contention is specifically admitted or traversed, the same may be treated as denied.

3. That at the very outset the answering Respondent respectfully submits that there is no merit in the present writ petition filed by the Petitioner herein. The alleged “facts”, on the basis which the Petitioner has filed the present petition are unsubstantiated statements and the information relating to the Aadhaar scheme has been grossly misreported and interpolated to mislead this Hon’ble Court. The Petitioner has pivoted his entire case around the misleading and unverified reports in the media regarding security breach of data related to Aadhaar, which is entirely denied as incorrect and misinformed.

PRELIMINARY OBJECTIONS-

4. That the preliminary objections raised by the Respondent herein to the present writ petition relate to the maintainability of the present writ petition. It is respectfully submitted that the present writ petition is not maintainable for two main reasons-
 - a) The writ petition is not maintainable after the judgment of Hon’ble Supreme Court in the case of Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors, W.P. (Civil) No. 494 / 2012, on validity of Aadhaar; and

b) Petitioner has no locus standi to file this petition.

c) The issues raised in the present writ petition are squarely covered by the judgment DATED 26.09.2018 of the Constitution Bench of Hon'ble Supreme Court in **K.S. PUTTASWAMY V UNION OF INDIA Writ Petition (Civil) No. 494/2012**

5. That as per the first paragraph of the Writ Petition filed by the Petitioner herein, the petition has been filed for "the redressal of the egregious violation of the Petitioner's right to privacy and dignity under Article 21 of the Constitution of India".

6. That the Petitioner herein has further made it clear in the writ petition that he is not challenging the constitutional validity of the Aadhaar Act, 2016 since a constitutional challenge was already pending before the Hon'ble Supreme Court. Further, when the matter came up for hearing before this Hon'ble Court on 18.05.2018, this Hon'ble Court was pleased to pass the following order-

"Counsel for the respondents, who appear on advance notice, state that the issues raised in the writ petition have been raised before the Supreme Court in Writ Petition (Civil) No. 494/2012, Justice K.S. Puttaswamy (Retd.) and Another versus Union of India and Others and other connected matters and judgment have been reserved.

Re-list on 21st August, 2018."

7. That at the very outset, it is submitted that the present petition is not maintainable and is liable to be dismissed in light of the judgment of the Constitution Bench decision of the Hon'ble Supreme Court of India in Justice K.S. Puttaswamy & Anr. Vs. Union of India & Ors. 2018 SCC

OnLine SC 1642 (hereinafter referred to as the “Aadhaar judgment”), wherein the Hon’ble Supreme Court has upheld the constitutional validity of the Aadhaar Act, 2016.

8. That the paragraph 16 of the writ petition deals with the “facts” allegedly giving rise to the present writ petition. Under paragraph 16 sub-paragraph (vii), the main headings under which the pleadings in the writ petition are arranged are given. The said paragraph is being reproduced here for this Hon’ble Court’s reference-

“vii. In order to make for an easier perusal of this petition, the pleadings are arranged under the following main headings:

(A) Security Breaches and Statutory Provisions Violated;

(B) Data Protection Duties under the law;

(C) Appointment of Investigative/Audit Committee;

(D) Constitutional/Common Law Rights and Damages;

(E) The Right to Know; and

(F) The Right to Legal Redressal.”

9. That it is respectfully submitted that all the above mentioned issues have been elaborately discussed and answered by the majority judgment of the Constitution Bench of Hon’ble Supreme Court and the grounds raised by the Petitioner in the present writ petition therefore have already been decided by the highest court of the land. Moreover, the Hon’ble Supreme Court has specifically tested the Aadhaar Act, 2016 against the right to privacy enshrined under Article 21, by applying the principles laid down by the 9 judge bench decision of the

Hon'ble Supreme Court in Justice K.S. Puttaswamy Vs. Union of India & Ors.(2017) 10 SCC 1.

10. That a plain reading of the following paragraph of the Aadhaar judgment, which lists out the issues decided by the Constitution Bench of Hon'ble Supreme Court demonstrates how the issues framed therein entirely cover the grounds raised by the Petitioner in the present writ petition -

“127. After setting the tone of the case, it is now time to specify the precise issues which are involved that need to be decided in these matters:

1. Whether the Aadhaar Project creates or has tendency to create surveillance state and is, thus, unconstitutional on this ground?

a) What is the magnitude of protection that needs to be accorded to collection, storage and usage of biometric data?

b) (b) Whether the Aadhaar Act and Rules provide such protection, including in respect of data minimisation, purpose limitation, time period for data retention and data protection and security?

2. Whether the Aadhaar Act violates right to privacy and is unconstitutional on this ground?

(This issue is considered in the context of Sections 7 and 8 of the Aadhaar Act. Incidental issue of 'Exclusion' is also considered here)

3. Whether children can be brought within the sweep of Sections 7 and 8 of the Aadhaar Act?

4. Whether the following provisions of the Aadhaar Act and Regulations suffer from the vice of unconstitutionality:

(i) Sections 2(c) and 2(d) read with Section 32

(ii) Section 2(h) read with Section 10 of CIDR

(iii) *Section 2(1) read with Regulation 23*

(iv) *Section 2(v)*

(v) *Section 3*

(vi) *Section 5*

(vii) *Section 6*

(viii) *Section 8*

(ix) *Section 9*

(x) *Sections 11 to 23*

(xi) *Sections 23 and 54*

(xii) *Section 23(2)(g) read with Chapter VI & VII-Regulations 27 to 32*

(xiii) *Section 29*

(xiv) *Section 33*

(xv) *Section 47*

(xvi) *Section 48*

(xvii) *Section 57*

(xviii) *Section 59*

(5) *Whether the Aadhaar Act defies the concept of Limited Government, Good Governance and Constitutional Trust?*

(6) *Whether the Aadhaar Act could be passed as 'Money Bill' within the meaning of Article 110 of the Constitution?*

(7) *Whether Section 139AA of the Income Tax Act, 1961 is violative of right to privacy and is, therefore, unconstitutional?*

(8) *Whether Rule 9(a)(17) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and the notifications issued thereunder, which mandate linking of Aadhaar with bank accounts, are unconstitutional?*

7

(9) Whether Circular dated March 23, 2017 issued by the Department of Telecommunications mandating linking of mobile number with Aadhaar is illegal and unconstitutional?

(10) Whether certain actions of the respondents are in contravention of the interim orders passed by the Court, if so, the effect thereof?"

11. That the Hon'ble Supreme Court, after examining the issues listed above in detail, inter alia, examined the validity of the Aadhar Act, 2016 under the provisions of the Constitution and specifically under Article 21 and the right to privacy emanating therefrom and upheld the Act while reading down certain provisions therein like Section 57.

12. It is submitted that the issues raised in the present writ petition were identical to the issues raised in the writ petition which were decided by the Supreme Court in the case of *KS Puttaswamy*. A plain reading of the of the affidavits filed, written submissions presented in court, additional documents placed on record of the Supreme Court show that the same issues were raised and considered by the Supreme Court while deciding the constitutional Validity of the Aadhaar Act 2016.

The following documents are being placed on record:-

a. "Additional Affidavit" filed by the Petitioners in S.G. Vombatkare&Anr. Vs. Union of India & ors. in W.P(C) No. 797 of 2016 dated 15.01.2018.

True Copy of Relevant extracts of the Additional Affidavit in W.P(C) No. 797 of 2016 dated 15.01.2018 is annexed and marked herewith as **Annexure R-1**.

b. "Application seeking permission to place certain Additional Documents on Record" filed by the Petitioners in Nachiketa Udupa

8

&Anr. Vs. Union of India & Ors. in W.P(C) No. 1056 of 2017 dated 12.01.2018.

True Copy of Relevant extracts of the Application seeking permission to place certain Additional Documents on Record in W.P(C) No. 1056 of 2017 dated 12.01.2018 is annexed and marked herewith as **Annexure R-2**.

- c. Written Submissions on behalf of Mr. K.V.Viswanathan, Sr. Adv. in Just. K.S. Puttaswamy&Anr. Vs. Union of India & Ors. Writ Petition (C) No. 494/2012.

True Copy of Relevant extracts of the Written Submissions on behalf of Mr. K.V.Viswanathan, Sr. Adv. in Writ Petition (C) No. 494/2012 is annexed and marked herewith as **Annexure R-3**.

- d. Compilation on behalf of Mr. K.V.Viswanathan, Sr., Adv., Vol.IV- 'Centralised Data Storage, Breach and Access', in Just. K.S. Puttaswamy&Anr. Vs. Union of India & Ors. Writ Petition (C) No. 494/2012.

True Copy of Relevant extracts of the Compilation on behalf of Mr. K.V.Viswanathan, Sr. Adv., Vol.IV- 'Centralised Data Storage, Breach and Access', in Writ Petition (C) No. 494/2012 is annexed and marked herewith as **Annexure R-4**.

- e. Written Submissions on behalf of Ms. Meenakshi Arora, Sr. Adv. in Just. K.S. Puttaswamy&Anr. Vs. Union of India & Ors. Writ Petition (C) No. 494/2012.

True Copy of Relevant extracts of the Written Submissions on behalf of Ms. Meenakshi Arora, Sr. Adv. in Writ Petition (C) No. 494/2012 is annexed and marked herewith as **Annexure R-5**

f. Written Submissions on behalf of Mr. Anand Grover, Sr. Adv. in Just. K.S. Puttaswamy & Anr. Vs. Union of India & Ors. Writ Petition (C) No. 494/2012.

True Copy of Relevant extracts of the Written Submissions on behalf of Mr. Anand Grover, Sr. Adv. in Writ Petition (C) No. 494/2012 is annexed and marked herewith as **Annexure R-6**.

g. That the answering Respondent had also filed an Additional Affidavit before the Hon'ble Supreme Court dated 09.03.2018 to answer the averments raised in several fresh affidavits filed while the matter was being heard by the Hon'ble Court which related to facts which have not been raised earlier and therefore it has become necessary to controvert those averments. The said affidavit specifically dealt with the following broad issues-

- i. **Allegations dealing with Exclusion**
- ii. **Allegations dealing with Data Security**
- iii. **Allegations dealing with Privacy & Surveillance**
- iv. **Allegations dealing with Inaccurate Claims qua Savings**

True Copy of the relevant extracts of the Additional Affidavit dated 09.03.2018 filed before the Hon'ble Supreme Court is annexed and marked herewith as **Annexure R-7**.

13. The Hon'ble Supreme Court has, on appreciating the rival submissions of the parties laid down the law in this regard. The Respondent herein seeks the liberty of this Hon'ble Court to extract and rely upon the following paragraphs of the Aadhaar judgment, as follows-

On Surveillance, Data Protection and Security-

“153. After going through the Aadhaar structure, as demonstrated by the respondents in the powerpoint presentation from the provisions of the Aadhaar Act and the machinery which the Authority has created for data protection, we are of the view that it is very difficult to create profile of a person simply on the basis of biometric and demographic information stored in CIDR. Insofar as authentication is concerned, the respondents rightly pointed out that there are sufficient safeguard mechanisms. To recapitulate, it was specifically submitted that there were security technologies in place (slide 28 of Dr. Pandey's presentation), 24/7 security monitoring, data leak prevention, vulnerability management programme and independent audits (slide 29) as well as the Authority's defence mechanism (slide 30). It was further pointed out that the Authority has taken appropriate proactive protection measures, which included disaster recovery plan, data backup and availability and media response plan (slide 31). The respondents also pointed out that all security principles are followed inasmuch as: (a) there is PKI-2048 encryption from the time of capture, meaning thereby, as soon as data is given at the time of enrolment, there is an end to end encryption thereof and it is transmitted to the Authority in encrypted form. The said encryption is almost foolproof and it is virtually impossible to decipher the same; (b) adoption of best-in-class security standards and practices; and (c) strong audit and traceability as well as fraud detection. Above all, there is an oversight of Technology and Architecture Review Board (TARB) and Security Review Committee. This Board and Committee consist of very high profiled officers. Therefore, the Act has endeavoured to provide safeguards⁶⁷.

...

197. Insofar as authentication process is concerned, that has already been taken note of above. The manner in which it is explained by the respondent authority, that may not pose much of a problem. **As noted earlier, while seeking authentication, neither the location of the person whose identity is to be verified nor the purpose for which authentication of such identity is needed, comes to the knowledge of the Authority and, therefore, such data collected by the Authority. Therefore, the threat to real time surveillance and profiling may be far-fetched.** The respondents

have explained that Section 2(d) defines “authentication record” to mean the record of the time of authentication, identity of the RE and the response provided by the authority”, Regulation 26(a) to (d) does not go beyond the scope of Section 2(d). None of the four clauses of Regulation 26 entitle the authority to store data about the purpose for which authentication is being done. The device can therefore only tell the authority the identity of the RE, the PID, the time and nature of response, the code of the device and the authentication server side configurations. Identity of the RE does not include details of the organization which is seeking authentication as an RE provides authentication service to large number of government organizations who have agreements with it. Such a mechanism preventing the authority from tracking the nature of activity for which the authentication was required. To illustrate nic.in is an RE which provides authentication service to large number of Government organisations who have agreements with it. The authentication record would only contain information about the identity about the RE. It will give information only about the RE (nic.in) and not about the organisation which is requiring authentication through the RE. In most cases the authentication is one time. Mr. Dwivedi has also explained that yet again, there may be organisations, which have branches in different part of India. Assuming Apollo Hospital (although in fact it is not an RE) has five branches in India. If Apollo Hospital seeks authentication as an RE, the authentication record will merely tell the identity of Apollo Hospital and its device code, but it will not indicate which branch of Apollo was seeking authentication and from which part of the country. Further, assuming that the Indira Gandhi International Airport is an RE and there is requirement of authentication at the point of entry and/or exit. All that the record will show that the ANH has entered the airport at a particular time but it will not show by which plane he is flying and to what destination. At the time of exit, it will only show that the person has exited the airport at a particular time. It will not show from which flight he has arrived and from which destination and at what time he has arrived or with whom he travelled.

...

207. The Respondents contend that strong measures for data protection and security, taken at all stages of data collection, transfer, storage and use.

After deliberating over respective contentions, we are of the opinion that the following explanation furnished by the respondents on various facets ensures data protection and security to a considerable extent:

(a) CIDR

208. Regulation 3(i) & (j) of Aadhaar (Data Security) Regulation 2016 enables partitioning of CIDR network into zones based on risk and trust and other security measures. CIDR being a computer resource is notified to be a “Protected System” under Section 70 of the IT Act, 2000 by the Central Government on 11.12.2015. Anyone trying to unlawfully gain access into this system is liable to be punished with 10 years imprisonment and fine. The storage involves end to end encryption, logical partitioning, firewalling and anonymisation of decrypted biometric data. Breaches of penalty are made punitive by Chapter VII of the Act. Biometric information is deemed to be an “electronic record”, and “Sensitive personal data or information” under the IT Act, 2000. There are further guards under The Aadhaar (Data Security) Regulation, 2016.

(b) Requesting Entities (AUA and KUA)

209. Other identity information is shared with Requesting Entity (AUAs and KUAs) only for the limited purpose of authentication. The data is transferred from the RE to the ASA (Authentication Service Agency) to the CIDR in an encrypted manner through a leased line circuitry using secure Protocols (Regulation 9 of the Authentication Regulations). The storage of data templates is in safely located servers with no public internet inlet/outlet, and offline storage of original encrypted data (PID blocks). There are safety and security provisions such as audit by Information Systems Auditor. REs are appointed through agreement. REs can enter into agreement with sub-AUA or sub-KUA with permission of the UIDAI. Whatever identity information is obtained by the requesting entity is based on a specific consent of the Aadhaar number holder. The e-KYC data shared with the RE can only be after prior consent of the Aadhaar holder. Such data cannot be shared and has to be stored in encrypted form. The biometric information used is not permitted to be stored only the logs of authentication transactions are maintained for a short period. Full identity information is never transmitted back to RE. There is a statutory bar from

sharing Biometric information [Section 29(1)(a)/Section 29(4)]. The Data centres of ASA, REs and CIDR should be within the territory of India.

(c) Enrolment Agencies and Registrars

210. The enrolment and Authentication processes are strongly regulated so that data is secure. The Enrolment agency, which collects the biometric and demographic of the individuals during enrolment, is appointed either by UIDAI or by a Registrar [Section 2(s)]. The registrar are appointed through MoUs or agreements for enrolment and are to abide by a code of conduct and processes, policies and guidelines issued by the authority. They are responsible for the process of enrolment. Categories of persons eligible for appointment are limited by the Regulations. The agency employees a certified supervisor, an operator and a verifier under Enrolment and Update Regulations. Registrars, enrolling agencies are obliged to use the software provided or authorized by UIDAI for enrolment purpose. The standard software has security features as specified by Authority. All equipment used are as per the specification issued by the authority. The Registrars are prohibited from using the information collected for any purpose other than uploading the information to CIDR. Sub-contracting of enrolment function is not allowed. The Code of Conduct contains specific directions for following the confidentiality, privacy and security protocols and submission of periodic reports of enrolment. Not only there are directions prohibiting manipulation and fraudulent practices but the Act contains penal provisions for such violations in Chapter VII of the Regulations. The enrolment agencies are empanelled by the authority. They are given an enrolling agency code using which the Registrar can onboard such agency to the CIDR. The enrolment data is uploaded to the Central Identities Data Repository (CIDR) certified equipment and software with a digital signature of the registrar/enrolling agency. The data is encrypted immediately upon capture. The decryption key is with the UIDAI solely. Section 2(ze) of the IT Act, which defines 'secure systems' and Section 2(w) of the Act, which defines 'intermediaries' apply to the process.

(d) Authentication Service Agency

211. Authentication only becomes available through the Authentication Service Agency (ASA). They are regulated by the Aadhaar

(Authentication) Regulations, 2016. Their role and responsibilities are provided by Authentication Regulation 19. They are to use certified devices, equipment, or software are duly registered with or approved or certified by the Authority/agency. The systems and operations are audited by information system auditor. The REs pass the encrypted data to the CIDR through the ASA and the response (Yes/No authentication or e-KYC information) also takes the same route back. The server of the ASA has to perform basic compliance and completeness checks on the authentication data packet before forwarding it to the CIDR.

(e) Hacking

212. As far as hacking is concerned, the respondents submit that the authority has involved adequate firewalling and other safety features. The biometric data stored in the CIDR is stored offline. Only templates are online. So far there has been no incidence of hacking. However, the authority is conscious of the hackers and it constantly updates itself to safeguard the data.

It may, however, be mentioned that of late certain reports have appeared in newspapers to the effect that some people could hack the website of CIDR, though it is emphatically denied by the UIDAI. Since there are only newspapers reports to this effect which appeared after the conclusion of hearing in these cases and, therefore, parties could not be heard on this aspect, we leave this aspect of the matter at that with a hope that CIDR would find out the ways and means to curb any such tendency.

(f) Biometric Solution Providers

213. With respect to foreign companies owning software, Respondents submit that UIDAI has entered into licensing agreements with foreign biometric solution providers (BSP) for software. Even though the source code of the software are retained by the BSP as it constitutes their Intellectual property, the data in the server rooms is secure as the software operates automatically and the biometric data is stored offline. There is no opportunity available to BSP to extract data as they have no access to it.

...

15

219. We are of the view that most of the apprehensions of the petitioners stand assuaged with the treatment which is given by us to some of the provisions. Some of these are already discussed above and some provisions are debated in the next issue. Summary thereof, however, can be given hereunder:

(a) Authentication records are not to be kept beyond a period of six months, as stipulated in Regulation 27(1) of the Authentication Regulations. This provision which permits records to be archived for a period of five years is held to be bad in law.

(b) Metabase (sic Metadata) relating to transaction, as provided in Regulation 26 of the aforesaid Regulations in the present form, is held to be impermissible, which needs suitable amendment.

(c) Section 33 of the Aadhaar Act is read down by clarifying that an individual, whose information is sought to be released, shall be afforded an opportunity of hearing.

(d) Insofar as Section 33(2) of the Act in the present form is concerned, the same is struck down.

(e) That portion of Section 57 of the Aadhaar Act which enables body corporate and individual to seek authentication is held to be unconstitutional.

(f) We have also impressed upon the respondents, as the discussion hereinafter would reveal, to bring out a robust data protection regime in the form of an enactment on the basis of Justice B.N. Srikrishna (Retd.) Committee Report with necessary modifications thereto as may be deemed appropriate.

220. With the removal of the aforesaid provisions from the statute and the Rules, coupled with the statement of the Authority on affidavit that there is no record of any transactions carried out by the individuals which is even known (and, therefore, no question of the same being retained by the Authority), most of the apprehensions of the petitioners are taken care of. At the same time, we may remind ourselves of the judgment in *G. Sundarrajan v. Union of India*⁷⁸. In that case, the Court noted the safety and security risk in the setting up of the nuclear power plant in the backdrop of

Fukushima disaster and Bhopal Gas tragedy. Yet, keeping in view the importance of generation of nuclear energy, the Court observed that a balance should be struck between production of nuclear energy which was of extreme importance for the economic growth, alleviation of poverty, generation of employment, and the smaller violation to right to life under Article 21. It took note of the opinion of experts committee and observed that 'adequate safety measure' have been taken. It noted huge expenditure of money running into crores and observed 'apprehension however legitimate it may be, cannot override the justification of the project. Nobody on this earth can predict what would happen in future and to a larger extent we have to leave it to the destiny. But once the justification test is satisfied, the apprehension test is bound to fail. Apprehension is something we anticipate with anxiety or fear, a fearful anticipation, which may vary from person to person'. The Court also held that 'nuclear power plant is being established not to negate right to life but to protect the right to life guaranteed under Article 21 of the Constitution. No doubt, the Court took a view that this interest of people needed to be respected for their human dignity which was divinity. However, it was also stressed that generation of nuclear energy was a nuclear necessity and the project was for larger public benefit and consequently, individual interest or smaller public interest must yield. In such a situation, necessity for 'adequate care, caution, and monitoring at every stage' and 'constant vigil' was emphasised. Safety and security was read into Article 21. Acknowledging that proportionality of risk may not be 'zero', regard being had to the nature's unpredictability, the Court ruled that all efforts must be made to avoid disaster by observing the highest degree of constant alertness. In the directions of the Court, it was observed that 'maintaining safety is an ongoing process not only at the design level but also during the operation'. In the present case as well, we have come to the conclusion that Aadhaar Act is a beneficial legislation which is aimed at empowering millions of people in this country. The justification of this project has been taken note of in detail, which the subsequent discussion shall also demonstrate. **In such a scenario only on apprehension, the project cannot be shelved.** At the same time, data protection and data safety is also to be ensured to avoid even the remote possibility of data profiling or data leakage.

221. Notwithstanding the statutory provision discussed above, we are of the view that there is a need for a proper legislative mechanism for data protection. The Government is not unmindful of this essential requirement. During the arguments it was stated by Mr. K.K. Venugopal, learned Attorney General, that an expert committee heading by Justice B.N. Srikrishna (Retd.) was constituted which was looking into the matter. The said Committee has since given its report.

222. In this behalf, it may be worthwhile to mention that one of the first comprehensive reports on data protection and informational privacy was prepared by the Group of Experts⁷⁹ constituted by the Planning Commission of India under the Chairmanship of Retd. Justice A.P. Shah, which submitted a report on 16 October, 2012. The five salient features of this report were expected to serve as a conceptual foundation for legislation protecting privacy. The framework suggested by the expert group was based on five salient features: (i) Technological neutrality and interoperability with international standards; (ii) Multi-Dimensional privacy; (iii) Horizontal applicability to state and non-state entities; (iv) Conformity with privacy principles; and (v) A co-regulatory enforcement regime.

223. The Union Government, on 31 July 2017, had constituted a committee chaired by Retd. Justice B N Srikrishna, former Judge of the Supreme Court of India to review data protection norms in the country and to make recommendations. The Committee recently released its report and the first draft of the *Personal Data Protection Bill, 2018* which comprehensively addresses the processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India. The bill has incorporated provisions and principles from the Europe's General Data Protection Regulation (EUGDPR).

...

229. The Srikrishna Committee Report and the Draft Data Protection Bill are the first articulation of a data protection law in our country. They have incorporated many of the progressive data protection principles inspired by the EUGDPR. There may be indeed be scope for further fine tuning of this law through a consultative process, however, we are not far away from a comprehensive data protection regime which entrenches informational and

data privacy within our laws and legal system. We hope that there would be a robust statutory regime in place in near future.

230. The aforesaid discussion leads us to hold that the protection that there is going to be a surveillance state created by the Aadhaar project is not well founded, and in any case, taken care of by the diffidence exercise carried out with the striking down certain offending provisions in their present form.

On Privacy-

260. Before we proceed to analyse the respective submissions, it has also to be kept in mind that all matters pertaining to an individual do not qualify as being an inherent part of right to privacy. Only those matters over which there would be a reasonable expectation of privacy are protected by Article 21. This can be discerned from the reading of Paras 297 to 307 of the judgment, relevant portions whereof have already been quoted above.

...

308. As against the above larger public interest, the invasion into the privacy rights of these beneficiaries is minimal. By no means it can be said that it has disproportionate effect on the right holder.

309. Intensity of review depends upon the particular context of question in a given case. There is yet another significant angle in these matters, which has to be emphasised at this stage viz. dignity in the form of autonomy (informational privacy) and dignity in the form of assuring better living standards, of the same individual. In the instant case, a holistic view of the matter, having regard to the detailed discussion hereinabove, would amply demonstrate that enrolment in Aadhaar of the unprivileged and marginalised section of the society, in order to avail the fruits of welfare schemes of the Government, actually amounts to empowering these persons. On the one hand, it gives such individuals their unique identity and, on the other hand, it also enables such individuals to avail the fruits of welfare schemes of the Government which are floated as socio-economic welfare measures to uplift such classes. In that sense, the scheme ensures dignity to such individuals. This facet of dignity cannot be lost sight of and needs to be acknowledged.

We are, by no means, accepting that when dignity in the form of economic welfare is given, the State is entitled to rob that person of his liberty. That can never be allowed. We are concerned with the balancing of the two facets of dignity. **Here we find that the inroads into the privacy rights where these individuals are made to part with their biometric information, is minimal. It is coupled with the fact that there is no data collection on the movements of such individuals, when they avail benefits under Section 7 of the Act thereby ruling out the possibility of creating their profiles. In fact, this technology becomes a vital tool of ensuring good governance in a social welfare state. We, therefore, are of the opinion that the Aadhaar Act meets the test of balancing as well.**

...

316. Needless to emphasise that when a law limits a constitutional right which many laws do, such limitation is constitutional if it is proportional. The law imposing restriction is proportional if it is meant to achieve a proper purpose, and if the measures taken to achieve such a purpose are rationally connected to the purpose, and such measures are necessary. Such limitations should not be arbitrary or of an excessive nature beyond what is required in the interest of the public. Reasonableness is judged with reference to the objective which the legislation seeks to achieve, and must not be in excess of that objective (see *P.P. Enterprises v. Union of India* [*P.P. Enterprises v. Union of India*, (1982) 2 SCC 33 : 1982 SCC (Cri) 341]). Further, the reasonableness is examined in an objective manner from the standpoint of the interest of the general public and not from the point of view of the person upon whom the restrictions are imposed or abstract considerations (see *Mohd. Hanif Quareshi v. State of Bihar* [*Mohd. Hanif Quareshi v. State of Bihar*, AIR 1958 SC 731]).”

317. Thus, even when two aspects of the fundamental rights of the same individual, which appear to be in conflict with each other, is done, we find that the Aadhaar Act has struck a fair balance between the right of privacy of the individual with right to life of the same individual as a beneficiary.

In the face of the all pervading prescript for accomplished socio-economic rights, that need to be given to the deprived and marginalised section of the

society, as the constitutional imperative embodied in these provisions of the Act, it is entitled to receive judicial imprimatur.

...

On Opting out-

376. There is yet another angle from which the matter can be looked into. In any case, when the Aadhaar scheme/project under the Act has been saved from the challenge to its constitutionality, we see no reason to invalidate the enrolments which were made prior to the passing of this Act as it would lead to unnecessary burden and exercise of enrolling these persons all over again. Instead the problem can be solved by eliciting 'consent' of all those persons who were enrolled prior to the passing of the Act. Since, we have held that enrolment is voluntary in nature, those who specifically refuse to give the consent, they would be allowed to exit from Aadhaar scheme. After all, by getting Aadhaar card, an individual so enrolled is getting a form of identity card. It would still be open to such an individual to make use of the said Aadhaar number or not. Those persons who need to avail any subsidy, benefit or service would need Aadhaar in any case. It would not be proper to cancel their Aadhaar cards. If direction is given to invalidate all those enrolments which were made prior to 2016 then such persons will have to undergo the rigours of getting themselves enrolled all over again. On the other hand, those who do not get any benefit of the nature prescribed under Section 7 of the Act, it would always be open for them not to make use of Aadhaar card or to make use of this card in a limited sense, namely, showing it as a proof of their identity, without undergoing any authentication process. Therefore, to a large extent, it does not harm this later category as well.

We, thus, uphold the validity of Section 59. As a corollary, Aadhaar for the period from 2009 to 2016 also stands validated.

...

Answer to the Issues raised in paragraph 127-

449. After stating the aforesaid manner in which different issues that arose are specified and discussed, these questions and conclusions thereupon are summarised below:

(1) *Whether the Aadhaar Project creates or has tendency to create surveillance state and is, thus, unconstitutional on this ground?*

Incidental Issues:

- (a) What is the magnitude of protection that need to be accorded to collection, storage and usage of biometric data?
- (b) Whether the Aadhaar Act and Rules provide such protection, including in respect of data minimisation, purpose limitation, time period for data retention and data protection and security?

Answer:

- (a) **The architecture of Aadhaar as well as the provisions of the Aadhaar Act do not tend to create a surveillance state. This is ensured by the manner in which the Aadhaar project operates.**
- (b) We have recorded in detail the powerpoint presentation that was given by Dr. Ajay Bhushan Pandey, CEO of the Authority, which brings out the following salient features:
 - (i) During the enrolment process, minimal biometric data in the form of iris and fingerprints is collected. The Authority does not collect purpose, location or details of transaction. Thus, it is purpose blind. The information collected, as aforesaid, remains in silos. Merging of silos is prohibited. The requesting agency is provided answer only in 'Yes' or 'No' about the authentication of the person concerned. The authentication process is not exposed to the Internet world. Security measures, as per the provisions of Section 29(3) read with Section 38(g) as well as Regulation 17(1)(d) of the Authentication Regulations, are strictly followed and adhered to.
 - (ii) There are sufficient authentication security measures taken as well, as demonstrated in Slides 14, 28 and 29 of the presentation.
 - (iii) The Authority has sufficient defence mechanism, as explained in Slide 30. It has even taken appropriate protection measures as demonstrated in Slide 31.

- (iv) There is an oversight by Technology and Architecture Review Board (TARB) and Security Review Committee.
 - (v) During authentication no information about the nature of transaction etc. is obtained.
 - (vi) The Authority has mandated use of Registered Devices (RD) for all authentication requests. With these, 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 the Authentication Regulations.
 - (vii) The Authority gets the AUA code, ASA code, unique device code, registered device code used for authentication. It does not get any information related to the IP address or the GPS location from where authentication is performed as these parameters are not part of authentication (v2.0) and e-KYC (v2.1) API. The Authority would only know from which device the authentication has happened, through which AUA/ASA etc. It 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 authority 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.
- (c) After going through the Aadhaar structure, as demonstrated by the respondents in the powerpoint presentation from the provisions of the Aadhaar Act and the machinery which the Authority has created for data protection, **we are of the view that it is very difficult to create profile of a person simply on the basis of biometric and**

demographic information stored in CIDR. Insofar as authentication is concerned, the respondents rightly pointed out that there are sufficient safeguard mechanisms. To recapitulate, it was specifically submitted that there were security technologies in place (slide 28 of Dr. Pandey's presentation), 24/7 security monitoring, data leak prevention, vulnerability management programme and independent audits (slide 29) as well as the Authority's defence mechanism (slide 30). It was further pointed out that the Authority has taken appropriate pro-active protection measures, which included disaster recovery plan, data backup and availability and media response plan (slide 31). The respondents also pointed out that all security principles are followed inasmuch as: (a) there is PKI-2048 encryption from the time of capture, meaning thereby, as soon as data is given at the time of enrolment, there is an end to end encryption thereof and it is transmitted to the Authority in encrypted form. The said encryption is almost foolproof and it is virtually impossible to decipher the same; (b) adoption of best-in-class security standards and practices; and (c) strong audit and traceability as well as fraud detection. Above all, there is an oversight of Technology and Architecture Review Board (TARB) and Security Review Committee. This Board and Committee consists of very high profiled officers. Therefore, the Act has endeavoured to provide safeguards.

- (d) Insofar as use and protection of data is concerned, having regard to the principles enshrined in various cases, Indian and foreign, the matter is examined from the stand point of data minimisation, purpose limitation, time period for data retention, data protection and security (*qua* CIDR, requisite entities, enrolment agencies and Registrars, authentication service agency, hacking, biometric solution providers, substantive procedural or judicial safeguards). After discussing the aforesaid aspect with reference to certain provisions of the Aadhaar Act, we are of the view that apprehensions of the petitioners stand assuaged with the striking down or reading down or clarification of some of the provisions, namely:

- (i) Authentication records are not to be kept beyond a period of six months, as stipulated in Regulation 27(1) of the Authentication Regulations. This provision which permits records to be archived for a period of five years is held to be bad in law.
- (ii) Metabase relating to transaction, as provided in Regulation 26 of the aforesaid Regulations in the present form, is held to be impermissible, which needs suitable amendment.
- (iii) Section 33(1) of the Aadhaar Act is read down by clarifying that an individual, whose information is sought to be released, shall be afforded an opportunity of hearing.
- (iv) Insofar as Section 33(2) of the Act in the present form is concerned, the same is struck down.
- (v) That portion of Section 57 of the Aadhaar Act which enables body corporate and individual to seek authentication is held to be unconstitutional. (vi) We have also impressed upon the respondents, to bring out a robust data protection regime in the form of an enactment on the basis of Justice B.N. Srikrishna (Retd.) Committee Report with necessary modifications thereto as may be deemed appropriate.

(2) *Whether the Aadhaar Act violates right to privacy and is unconstitutional on this ground?*

Answer:

- (a) After detailed discussion, it is held that all matters pertaining to an individual do not qualify as being an inherent part of right to privacy. Only those matters over which there would be a reasonable expectation of privacy are protected by Article 21. This can be discerned from the reading of Paras 297 to 307 of the judgment.
- (b) **The Court is also of the opinion that the triple test laid down in order to adjudge the reasonableness of the invasion to privacy has been made. The Aadhaar scheme is backed by the statute, i.e. the Aadhaar Act. It also serves legitimate State aim, which can be discerned from the Introduction to the Act as well as the**

Statement of Objects and Reasons which reflect that the aim in passing the Act was to ensure that social benefit schemes reach the deserving community. The Court noted that the failure to establish identity of an individual has proved to be a major hindrance for successful implementation of those programmes as it was becoming difficult to ensure that subsidies, benefits and services reach the unintended beneficiaries in the absence of a credible system to authenticate identity of beneficiaries. The Statement of Objects and Reasons also discloses that over a period of time, the use of Aadhaar number has been increased manifold and, therefore, it is also necessary to take measures relating to ensuring security of the information provided by the individuals while enrolling for Aadhaar card.

- (c) It may be highlighted that the petitioners are making their claim on the basis of dignity as a facet of right to privacy. On the other hand, Section 7 of the Aadhaar Act is aimed at offering subsidies, benefits or services to the marginalised section of the society for whom such welfare schemes have been formulated from time to time. That also becomes an aspect of social justice, which is the obligation of the State stipulated in Para IV of the Constitution. The rationale behind Section 7 lies in ensuring targeted delivery of services, benefits and subsidies which are funded from the Consolidated Fund of India. In discharge of its solemn Constitutional obligation to enliven the Fundamental Rights of life and personal liberty (Article 21) to ensure Justice, Social, Political and Economic and to eliminate inequality (Article 14) with a view to ameliorate the lot of the poor and the Dalits, the Central Government has launched several welfare schemes. Some such schemes are PDS, scholarships, mid day meals, LPG subsidies, etc. These schemes involve 3% percentage of the GDP and involve a huge amount of public money. Right to receive these benefits, from the point of view of those who deserve the same, has now attained the status of fundamental right based on the same concept of human dignity, which the petitioners seek to bank upon. The Constitution does not exist for a few or minority of the people of India, but “We the people”. The goals set out in the

Preamble of the Constitution do not contemplate statism and do not seek to preserve justice, liberty, equality and fraternity for those who have the means and opportunity to ensure the exercise of inalienable rights for themselves. These goals are predominantly or at least equally geared to “secure to all its citizens”, especially, to the downtrodden, poor and exploited, justice, liberty, equality and “to promote” fraternity assuring dignity. Interestingly, the State has come forward in recognising the rights of deprived section of the society to receive such benefits on the premise that it is their fundamental right to claim such benefits. It is acknowledged by the respondents that there is a paradigm shift in addressing the problem of security and eradicating extreme poverty and hunger. The shift is from the welfare approach to a right based approach. As a consequence, right of everyone to adequate food no more remains based on Directive Principles of State Policy (Art 47), though the said principles remain a source of inspiration. This entitlement has turned into a Constitutional fundamental right. This Constitutional obligation is reinforced by obligations under International Convention.

- (d) Even the petitioners did not seriously question the purpose and *bona fides* of the Legislature enacting the law.
- (e) The Court also finds that the Aadhaar Act meets the test of proportionality as the following components of proportionality stand satisfied:
 - (i) A measure restricting a right must have a legitimate goal (legitimate goal stage).
 - (ii) It must be a suitable means of furthering this goal (suitability or rationale connection stage).
 - (iii) There must not be any less restrictive but equally effective alternative (necessity stage).
 - (iv) The measure must not have a disproportionate impact on the right holder (balancing stage).

- (f) In the process, the Court has taken note of various judgments pronounced by this Court pertaining to right to food, issuance of BPL Cards, LPG connections and LPG cylinders at minimal cost, old age and other kind of pensions to deserving persons, scholarships and implementation of MGNREGA scheme.
- (g) The purpose behind these orders was to ensure that the deserving beneficiaries of the scheme are correctly identified and are able to receive the benefits under the said scheme, which is their entitlement. The orders also aimed at ensuring 'good governance' by bringing accountability and transparency in the distribution system with the pious aim in mind, namely, benefits actually reached those who are rural, poor and starving.
- (h) All this satisfies the necessity stage test, particularly in the absence of any less restrictive but equally effective alternative.
- (i) Insofar as balancing is concerned, the matter is examined at two levels:
 - (i) Whether, 'legitimate state interest' ensures 'reasonable tailoring'?
There is a minimal intrusion into the privacy and the law is narrowly framed to achieve the objective. Here the Act is to be tested on the ground that whether it is found on a balancing test that the social or public interest and the reasonableness of the restrictions outweigh the particular aspect of privacy, as claimed by the petitioners. This is the test we have applied in the instant case.
 - (ii) There needs to be balancing of two competing fundamental rights, right to privacy on the one hand and right to food, shelter and employment on the other hand. Axiomatically both the rights are founded on human dignity. At the same time, in the given context, two facets are in conflict with each other. The question here would be, when a person seeks to get the benefits of welfare schemes to which she is entitled to as a part of right to live life with dignity, whether her sacrifice to the right to privacy, is so invasive that it creates imbalance?

- (j) In the process, sanctity of privacy in its functional relationship with dignity is kept in mind where it says that legitimate expectation of privacy may vary from intimate zone to the private zone and from the private to public arena. Reasonable expectation of privacy is also taken into consideration. **The Court finds that as the information collected at the time of enrolment as well as authentication is minimal, balancing at the first level is met. Insofar as second level, namely, balancing of two competing fundamental rights is concerned, namely, dignity in the form of autonomy (informational privacy) and dignity in the form of assuring better living standards of the same individual, the Court has arrived at the conclusion that balancing at the second level is also met.** The detailed discussion in this behalf amply demonstrates that enrolment in Aadhaar of the unprivileged and marginalised section of the society, in order to avail the fruits of welfare schemes of the Government, actually amounts to empowering these persons. On the one hand, it gives such individuals their unique identity and, on the other hand, it also enables such individuals to avail the fruits of welfare schemes of the Government which are floated as socio-economic welfare measures to uplift such classes. In that sense, the scheme ensures dignity to such individuals. This facet of dignity cannot be lost sight of and needs to be acknowledged. We are, by no means, accepting that when dignity in the form of economic welfare is given, the State is entitled to rob that person of his liberty. That can never be allowed. We are concerned with the balancing of the two facets of dignity. Here we find that the inroads into the privacy rights where these individuals are made to part with their biometric information, is minimal. It is coupled with the fact that there is no data collection on the movements of such individuals, when they avail benefits under Section 7 of the Act thereby ruling out the possibility of creating their profiles. In fact, this technology becomes a vital tool of ensuring good governance in a social welfare state. We, therefore, are of the opinion that the Aadhaar Act meets the test of balancing as well.

- (k) Insofar as the argument based on probabilistic system of Aadhaar, leading to 'exclusion' is concerned, the Authority has claimed that biometric accuracy is 99.76% and the petitioners have also proceeded on that basis. In this scenario, if the Aadhaar project is shelved, 99.76% beneficiaries are going to suffer. Would it not lead to their exclusion? It will amount to throwing the baby out of hot water along with the water. In the name of 0.232% failure (which can in any case be remedied) should be revert to the pre-Aadhaar stage with a system of leakages, pilferages and corruption in the implementation of welfare schemes meant for marginalised section of the society, the full fruits thereof were not reaching to such people?
- (l) The entire aim behind launching this programme is the 'inclusion' of the deserving persons who need to get such benefits. When it is serving much larger purpose by reaching hundreds of millions of deserving persons, it cannot be crucified on the unproven plea of exclusion of some. It is clarified that the Court is not trivialising the problem of exclusion if it is there. However, what we are emphasising is that remedy is to plug the loopholes rather than axe a project, aimed for the welfare of large section of the society. Obviously, in order to address the failures of authentication, the remedy is to adopt alternate methods for identifying such persons, after finding the causes of failure in their cases. We have chosen this path which leads to better equilibrium and have given necessary directions also in this behalf, viz:
- (i) We have taken on record the statement of the learned Attorney General that no deserving person would be denied the benefit of a scheme on the failure of authentication.
- (ii) We are also conscious of the situation where the formation of fingerprints may undergo change for various reasons. It may happen in the case of a child after she grows up; it may happen in the case of an individual who gets old; it may also happen because of damage to the fingers as a result of accident or some disease etc. or because of suffering of some kind of disability for

whatever reason. Even iris test can fail due to certain reasons including blindness of a person. We again emphasise that no person rightfully entitled to the benefits shall be denied the same on such grounds. It would be appropriate if a suitable provision be made in the concerned regulations for establishing an identity by alternate means, in such situations.

(m) As far as subsidies, services and benefits are concerned, their scope is not to be unduly expanded thereby widening the net of Aadhaar, where it is not permitted otherwise. In this respect, it is held as under:

- (i) 'Benefits' and 'services' as mentioned in Section 7 should be those which have the colour of some kind of subsidies etc., namely, welfare schemes of the Government whereby Government is doling out such benefits which are targeted at a particular deprived class.
- (ii) It would cover only those 'benefits' etc. the expenditure thereof has to be drawn from the Consolidated Fund of India.
- (iii) On that basis, CBSE, NEET, JEE, UGC etc. cannot make the requirement of Aadhaar mandatory as they are outside the purview of Section 7 and are not backed by any law.

(3) *Whether children can be brought within the sweep of Sections 7 and 8 of the Aadhaar Act?*

Answer:

- (a) For the enrolment of children under the Aadhaar Act, it would be essential to have the consent of their parents/guardian.
- (b) On attaining the age of majority, such children who are enrolled under Aadhaar with the consent of their parents, shall be given the option to exit from the Aadhaar project if they so choose in case they do not intend to avail the benefits of the scheme.
- (c) Insofar as the school admission of children is concerned, requirement of Aadhaar would not be compulsory as it is neither a service nor subsidy. Further, having regard to the fact that a

child between the age of 6 to 14 years has the fundamental right to education under Article 21A of the Constitution, school admission cannot be treated as 'benefit' as well.

(d) Benefits to children between 6 to 14 years under *Sarv Shiksha Abhiyan*, likewise, shall not require mandatory Aadhaar enrolment.

(e) For availing the benefits of other welfare schemes which are covered by Section 7 of the Aadhaar Act, though enrolment number can be insisted, it would be subject to the consent of the parents, as mentioned in (a) above.

(f) We also clarify that no child shall be denied benefit of any of these schemes if, for some reasons, she is not able to produce the Aadhaar number and the benefit shall be given by verifying the identity on the basis of any other documents. This we say having regard to the statement which was made by Mr. K.K. Venugopal, learned Attorney General for India, at the Bar.

(4) *Whether the following provisions of the Aadhaar Act and Regulations suffer from the vice of unconstitutionality:*

(i) Sections 2(c) and 2(d) read with Section 32

(ii) Section 2(h) read with Section 10 of CIDR

(iii) Section 2(l) read with Regulation 23

(iv) Section 2(v)

(v) Section 3

(vi) Section 5

(vii) Section 6

(viii) Section 8

(ix) Section 9

(x) Sections 11 to 23

(xi) Sections 23 and 54

(xii) Section 23(2)(g) read with Chapter VI & VII - Regulations 27 to 32

(xiii) Section 29

(xiv) Section 33

(xv) Section 47

(xvi) Section 48

(xvii) Section 57

(xviii) Section 59

Answer:

- (a) Section 2(d) which pertains to authentication records, such records would not include metadata as mentioned in Regulation 26(c) of the Aadhaar (Authentication) Regulations, 2016. Therefore, this provision in the present form is struck down. Liberty, however, is given to reframe the regulation, keeping in view the parameters stated by the Court.
- (b) Insofar as Section 2(b) is concerned, which defines 'resident', the apprehension expressed by the petitioners was that it should not lead to giving Aadhaar card to illegal immigrants. We direct the respondent to take suitable measures to ensure that illegal immigrants are not able to take such benefits.
- (c) Retention of data beyond the period of six months is impermissible. Therefore, Regulation 27 of Aadhaar (Authentication) Regulations, 2016 which provides archiving a data for a period of five years is struck down.
- (d) Section 29 in fact imposes a restriction on sharing information and is, therefore, valid as it protects the interests of Aadhaar number holders. However, apprehension of the petitioners is that this provision entitles Government to share the information 'for the purposes of as may be specified by regulations'. The Aadhaar (Sharing of Information) Regulations, 2016, as of now, do not contain any such provision. If a provision is made in the regulations which impinges upon the privacy rights of the Aadhaar card holders that can always be challenged.

- (e) Section 33(1) of the Act prohibits disclosure of information, including identity information or authentication records, except when it is by an order of a court not inferior to that of a District Judge. We have held that this provision is to be read down with the clarification that an individual, whose information is sought to be released, shall be afforded an opportunity of hearing. If such an order is passed, in that eventuality, he shall also have right to challenge such an order passed by approaching the higher court. During the hearing before the concerned court, the said individual can always object to the disclosure of information on accepted grounds in law, including Article 20(3) of the Constitution or the privacy rights etc.
- (f) Insofar as Section 33(2) is concerned, it is held that disclosure of information in the interest of national security cannot be faulted with. However, for determination of such an eventuality, an officer higher than the rank of a Joint Secretary should be given such a power. Further, in order to avoid any possible misuse, a Judicial Officer (preferably a sitting High Court Judge) should also be associated with. We may point out that such provisions of application of judicial mind for arriving at the conclusion that disclosure of information is in the interest of national security, are prevalent in some jurisdictions. In view thereof, Section 33(2) of the Act in the present form is struck down with liberty to enact a suitable provision on the lines suggested above.
- (g) Insofar as Section 47 of the Act which provides for the cognizance of offence only on a complaint made by the Authority or any officer or person authorised by it is concerned, it needs a suitable amendment to include the provision for filing of such a complaint by an individual/victim as well whose right is violated.
- (h) Insofar as Section 57 in the present form is concerned, it is susceptible to misuse inasmuch as: (a) It can be used for establishing the identity of an individual 'for any purpose'. We read down this provision to mean that such a purpose has to be backed by law. Further, whenever any such "law" is made, it would be subject to

judicial scrutiny. (b) Such purpose is not limited pursuant to any law alone but can be done pursuant to 'any contract to this effect' as well. This is clearly impermissible as a contractual provision is not backed by a law and, therefore, first requirement of proportionality test is not met. (c) Apart from authorising the State, even 'any body corporate or person' is authorised to avail authentication services which can be on the basis of purported agreement between an individual and such body corporate or person. Even if we presume that legislature did not intend so, the impact of the aforesaid features would be to enable commercial exploitation of an individual biometric and demographic information by the private entities. Thus, this part of the provision which enables body corporate and individuals also to seek authentication, that too on the basis of a contract between the individual and such body corporate or person, would impinge upon the right to privacy of such individuals. This part of the section, thus, is declared unconstitutional.

(i) Other provisions of Aadhaar Act are held to be valid, including Section 59 of the Act which, according to us, saves the pre-enactment period of Aadhaar project, i.e. from 2009-2016.

(5) Whether the Aadhaar Act defies the concept of Limited Government, Good Governance and Constitutional Trust?

Answer:

Aadhaar Act meets the concept of Limited Government, Good Governance and Constitutional Trust.

...

(7) Whether Section 139AA of the Income Tax Act, 1961 is violative of right to privacy and is, therefore, unconstitutional?

Answer:

Validity of this provision was upheld in the case of *Binoy Viswam* by repelling the contentions based on Articles 14 and 19 of the Constitution. The question of privacy which, at that time, was traced to Article 21, was left open. The matter is reexamined on the touchstone of

principles laid down in *K.S. Puttaswamy*. The matter has also been examined keeping in view that manifest arbitrariness is also a ground of challenge to the legislative enactment. Even after judging the matter in the context of permissible limits for invasion of privacy, namely: (i) the existence of a law; (ii) a 'legitimate State interest'; and (iii) such law should pass the 'test of proportionality', we come to the conclusion that all these tests are satisfied. In fact, there is specific discussion on these aspects in *Binoy Viswam's case* as well.

(8) *Whether Rule 9 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and the notifications issued thereunder which mandates linking of Aadhaar with bank accounts is unconstitutional?*

Answer:

- (a) We hold that the provision in the present form does not meet the test of proportionality and, therefore, violates the right to privacy of a person which extends to banking details.
- (b) This linking is made compulsory not only for opening a new bank account but even for existing bank accounts with a stipulation that if the same is not done then the account would be deactivated, with the result that the holder of the account would not be entitled to operate the bank account till the time seeding of the bank account with Aadhaar is done. This amounts to depriving a person of his property. We find that this move of mandatory linking of Aadhaar with bank account does not satisfy the test of proportionality. To recapitulate, the test of proportionality requires that a limitation of the fundamental rights must satisfy the following to be proportionate: (i) it is designated for a proper purpose; (ii) measures are undertaken to effectuate the limitation are rationally connected to the fulfilment of the purpose; (iii) there are no alternative less invasive measures; and (iv) there is a proper relation between the importance of achieving the aim and the importance of limiting the right.
- (c) The Rules are held to be disproportionate for the reasons stated in the main body of this Judgment.

(9) *Whether Circular dated March 23, 2017 issued by the Department of Telecommunications mandating linking of mobile number with Aadhaar is illegal and unconstitutional?*

Answer:

Circular dated March 23, 2017 mandating linking of mobile number with Aadhaar is held to be illegal and unconstitutional as it is not backed by any law and is hereby quashed.

(10) **Whether certain actions of the respondents are in contravention of the interim orders passed by the Court, if so, the effect thereof?**

Answer:

This question is answered in the negative.”

14. That therefore, the decision of the Hon’ble Apex Court as quoted above, has settled all the issues raised in the present writ petition and has declared the law on these issues under Article 141 of the Constitution. Accordingly, the present writ petition deserves to be dismissed with costs by this Hon’ble Court.

II. PETITIONER HAS NO LOCUS STANDI TO FILE THE PRESENT WRIT PETITION OR TO CLAIM DAMAGES-

15. It is humbly submitted that not only is the present writ petition devoid of merit, but also the Petitioner lacks the locus to file the present petition. Petitioner has alleged that “apart from being personally aggrieved, the Petitioner is filing the present writ petition in the interest of general public as well since many others have also signed up for a new age digital leash called “Aadhaar” and are likely to be similarly aggrieved”.

16. The petitioner has not been able to substantiate any grounds or facts to demonstrate how personal data pertaining to the petitioner has been breached and accordingly the petitioner has failed miserably to demonstrate any grievance whatsoever apart from making generalised sweeping statements about the Aadhaar project and the Aadhaar Act, both of which have been upheld by the Supreme Court. The petitioner is trying to re-agitate the same issues which have attained finality before the Supreme Court and therefore the present petition deserves to be dismissed with costs. It is vehemently denied that the Petitioner is aggrieved by the Aadhaar Act 2016 and its implementation in any manner whatsoever. Moreover, he claims to have filed the present petition on the presumption that others who have signed up for Aadhaar “are likely to be similarly aggrieved”. It is humbly submitted that, a writ petition cannot be filed on mere apprehension, without any real threat to the rights of the Petitioner. Secondly, a writ petition based on a mere assumption that the general public is likely to be aggrieved, cannot be entertained by the Court and therefore deserves to be dismissed with exemplary cost.
17. It is respectfully submitted that in the entire petition, there is not even a mention as to how the Petitioner is aggrieved by the actions of the Respondents and how his constitutional rights have been violated to entitle him to damages claimed by him.
18. Petitioner has, on the contrary admitted under Ground “B” of the petition that he does not even have knowledge of any damage caused to him and others and has therefore sought appointment of an independent committee “to investigate the scope and extent of breaches and the

magnitude of harm, both current and future.” Further, in Ground “C”, the petitioner has alleged that the data breaches have caused severe mental agony and emotional suffering to the Petitioner as he “fears potential misuse of his data at the hands of unscrupulous third parties”. The Petitioner has further averred that he reserves the liberty to seek appropriate compensation from the Respondents for all existing and future security risks arising out of the issue. Further, under Ground “G”, Petitioner has falsely and baselessly alleged that his Aadhaar number and other demographic and other details are now in possession of unauthorized third parties and therefore sought to opt out of Aadhaar system or in the alternative, the Respondents be directed to issue a new Aadhaar number to the Petitioner.

19. Based on the grounds above mentioned and several other baseless grounds, Petitioner has inter alia sought payment of exemplary damages to him in order to deter the Respondents from “future negligent behaviour”.
20. Respondent respectfully submits that the entire claim of the Petitioner is based on mere apprehensions and speculations and there is no merit in the present writ petition.
21. It is humbly submitted that none of the grounds raised by the Petitioner merit consideration by this Hon’ble Court. Petitioner seeks to hold the Respondents responsible on the basis of unsubstantiated news reports and on conjectures and surmises.
22. Moreover, on the basis of such frivolous and uncorroborated grounds, Petitioner seeks exemplary damages from the Respondent authorities. It is humbly submitted that Petitioner has not made out any case for

grant of any damages as no injury whatsoever has been caused to the Petitioner.

23. Therefore, it is the humble submission of the answering Respondent that the writ petition should be dismissed with exemplary costs.

I. REPLY TO THE AVERMENTS IN THE PRESENT WRIT PETITION

24. As submitted in the above paragraphs, the present writ petition is not maintainable and deserves to be dismissed *in limine*. However, by way of abundant caution, the answering Respondents seeks to answer the averments made by the Petitioner as follows-

25. Petitioner claims to have filed the present writ petition for the redressal of violation of his right to privacy under Article 21. As stated earlier, this issue has already been argued extensively before the Constitution Bench of the Hon'ble Supreme Court in Aadhaar judgment wherein, it has been held that all matters pertaining to an individual do not qualify as being an inherent part of right to privacy and only those matters over which there would be a reasonable expectation of privacy are protected by Article 21. The Court laid down the triple test which need to be satisfied for judging the permissible limits for invasion of privacy while testing the validity of any legislation. These are: (a) The existence of a law. (b) A "legitimate State interest"; and (c) Such law should pass the "test of proportionality". As stated earlier, the Hon'ble Supreme Court has it is

held that the architecture of Aadhaar as well as the provisions of the Aadhaar Act do not tend to create a surveillance state.

Requirement of Making Aadhaar Mandatory under the Law for delivery of welfare subsidies, benefits and services, income tax, bank accounts etc. -

26. With regard to the requirement of Making Aadhaar Mandatory under the Law for delivery of welfare subsidies, benefits and services, income tax, bank accounts etc. , it is humbly submitted that the Aadhaar Act makes Aadhaar mandatory for delivery of benefits, services and subsidies funded from the Consolidated fund of India. Section 7 of the Aadhaar Act which requires Aadhaar for the purpose of verification of the identity of the beneficiary of benefits, services and subsidies funded from the Consolidated fund of India has been upheld by the Supreme Court of India. The basic purpose of Aadhaar is to confirm the identity of the person to whom the benefit is targeted to be given. It was not so long ago, that huge sums of money in welfare schemes meant for poor were being siphoned away through duplicates and as a result genuine beneficiaries suffered. Ghosts and fakes in PAN, bank accounts, shell companies helped in large-scale tax evasion, money laundering, and generation of black money. All efforts of the government to weed out these ghosts from time to time had only a limited and transient impact as ghosts were so resilient that sooner than later, they used to reappear in much larger numbers. It was precisely to address this malaise that Aadhaar was conceptualized and was given a statutory basis in 2016 through the enactment of the Aadhaar Act, which enables the

government to make Aadhaar mandatory for welfare schemes and services.

27. The object of the Aadhaar Act i.e. the efficient, transparent and targeted delivery of subsidies, benefits and services to genuine beneficiaries is in furtherance of various facets of Article 21 of the poor people of India and also in furtherance of the Directive Principles of State Policy inter alia Articles 38, 39, 41, 43, 47 and 48. [Ref: Statement of Objects & Reasons of the Act]
28. It was seen that historically, respective governments allocated trillions of Rupees almost 3% of the GDP towards subsidies, scholarships, pensions, education and other welfare programs. But it was seen that nearly half of it never reached the intended beneficiaries. [Page 7 of the Common Additional Affidavit (CAA) dated 16.01.2018 placed before the Supreme Court of India]
29. A former Prime Minister had famously said that out of Rs 100 allocated to an anti-poverty project, only Rs 15 reaches the people, which was later confirmed by subsequent reports of Planning Commission.
30. Several studies initiated by the Government as well as the World Bank and Planning Commission revealed that food grains did not reach beneficiaries and that there was large scale leakages due to the failure to establish identity.
31. The Comptroller and Auditor General of India in its Audit Report No. 3 of 2000 for the year ended March, 1999 made a performance appraisal of various Centrally Sponsored/funded Schemes. One of the four schemes that were audited under the scope of this Report was the

Public Distribution Scheme under the Ministry of Food and Consumer Affairs. The CAG in its overview for the Audit Report observed that the programme suffered from serious targeting problems. The following findings were made by the CAG:-

- a. A significant portion of the subsidized foodgrains and other essential commodities did not reach the beneficiaries due to their diversion in the open market. [Page 8 r/w 215 of CAA]
- b. 18.47 Lakh tonne of foodgrains were diverted to purposes not connected with PDS. [Page 9 r/w 216 of CAA]
- c. **1.93 Crore bogus ration cards** were found to be in circulation in 13 states. Circulation of over 1.93 Crore bogus ration cards was noticed in 13 states leading to possibility of large scale diversions to open markets, excess drawal of foodgrains, sugar, etc. [Page 11 r/w 217 of CAA] [Refer to Page 268 for State-wise bogus ration cards]
- d. Proliferation of bogus ration cards was also cited as one of the deficiencies by the Programme Evaluation Organisation under the Planning Commission. [Refer to Page 12 r/w 222 CAA]

32. A Report titled Budgetary Subsidies in India – Subsidizing Social and Economic Services” prepared by the National Institute of Public Finance and Policy dated March, 2003 made the following findings:

- i. Better targeting is the key to lowering the volume of subsidy while continuing to satisfy the objectives of subsidization. [Refer to Page 13 r/w 309 (Vol-II) CAA]
- ii. With inadequate targeting, much of subsidised kerosene leaks to unintended beneficiaries/uses. Estimates in 1996 indicate that only 70 percent of the kerosene (domestic) distributed through this mechanism reached the poorer sections of society (Economic Survey, 2001). . [Refer to Page 14 r/w 299 (Vol-II) CAA]

33. A Report titled “Budget Briefs: Targeted Public Distribution System (TPDS), GOI 2011-2012” prepared by AvaniKapur and Anirvan

Chowdhury and published by the Accountability Initiative relying upon government reported data has made the following observations:

- i. There are a large number of ineligible/fake ration cards issued causing inefficiencies in targeting.
- ii. Between July 2006 and July 2010, in Bihar, Madhya Pradesh, Uttar Pradesh and Orissaa total of **37 Lakh ineligible/fake ration** cards for households have been eliminated.
- iii. Additionally, in Maharashtra and Madhya Pradesh **29 Lakh and 25 Lakh ineligible ration cards** were discovered and cancelled. [Refer to **Page 15 r/w 318** (Vol-II) CAA]

34. A Report prepared by the V.V. Giri National Labour Institute and sponsored by the Department of Rural Development, Ministry of Rural Development, Government of India titled as "The Study of Schedule of Rates for National Rural Employment Guarantee Scheme" observes that there was **great fraud in making fake cards** and it was found that in many cases, it was found that workers performed one day's job, but their attendance was put for 33 days. The workers got money for one day while wages for 32 days were misappropriated by the people associated with the functioning of NREGS.

[Refer to **Page 16 r/w 337** (Vol-II) CAA]

35. The World Bank with the aim of analyzing the impact on poor households of India's Public Distribution System(PDS) in terms of income gains, reduction in the incidence and severity of poverty as well as nutritional improvements published Discussion Paper No. 380 titled "India's Public Distribution System: A National and International Perspective" dated November, 1997 co-authored by R. Radhakrishna and K. Subbarao made the following findings:

- i. The income transfer to the poor in 1986-87 was estimated to be Rs 2840 million and the central government expenditure required to transfer one rupee worked out to Rs 4.27. The high cost is largely due to leakages to nonpoor, since the share of the poor in the total income gain was only 34 percent, and due to systemic inefficiencies (leakages due to pilferage, etc.). [Refer to **Page 17 r/w 348 (Vol-II) CAA**]
36. The Planning Commission of India in its Performance Evaluation Report titled "Performance Evaluation Report of Targeted Public Distribution System(TPDS)" dated March, 2005 found that about **58% of the subsidized food grains issued form the Central Pool do not reach the BPL families because of identification errors, non-transparent operation and unethical practices in the implementation of TPDS. The relevant findings are as follows:-**
- i. State-wise figure of excess Ration Cards in various states and notes the **existence of over 1.52 Crore excess Ration Cards issued.** [Page 362 of CAA]
 - ii. The Report also finds **fictitious households** and observes that identification errors lead to **exclusion of genuine beneficiaries.**
 - iii. It is further observed that **leakage through ghost BPL Ration Cards are found to be prevalent in almost all the states under study.** [Pg. 369 of CAA]
 - iv. The **Leakage of food grains through ghost cards** has been tabulated and the percentage of such leakage on an All India basis has been estimated at **16.67 %.** [Pg 370 of CAA]
 - v. It is concluded that a large part of the subsidized food-grains were not reaching the target group.
37. The Thirteenth Finance Commission Report for 2010-2015 dated December, 2009 at Page 218 in "Chapter 12 – Grants in Aid" states that the creation of a biometric-based unique identity for all residents in

the country has the potential to address need of the government to ensure that only eligible persons are provided subsidies and benefits and that all eligible persons are covered. The relevant findings are as follows:-

- i. Government of India's expenditure on subsidies is expected to be about Rs. 1,11,000 Crore in 2009-10, or nearly 18 per cent of the non-plan revenue expenditure. [Pg 22 r/w 418 of CAA]
 - ii. The data base of eligible persons presently maintained has both Type I (exclusion) and Type II (inclusion) errors. The first error arises from the difficulty faced by the poor in establishing their identity in order to be eligible for government subsidies and social safety net programmes. The second error arises because of the inability to cross-verify lists of eligible persons across district-level and state-level data bases to eliminate duplicate and ghost entries. We need to ensure that only eligible persons are provided subsidies and benefits and that all eligible persons are covered. [Pg 22 r/w 418 of CAA]
 - iii. **Creation of a biometric-based unique identity for all residents in the country has the potential to address both these dimensions simultaneously.** It will provide the basis for focusing subsidies to target groups. Possession of such an identity will also enable the poor and underprivileged to leverage other resources like bank accounts, cell phones, which can empower them and catalyse their income growth. These benefits cannot be accessed by them presently due to their inability to provide acceptable identification. The initiative to provide unique IDs has the potential to significantly improve the governance and delivery framework of public services while substantially reducing transaction costs, leakages and frauds. [Pg 22/23 r/w 418-419 of CAA]
38. The National Institute of Public Finance and Policy's report titled as "A Cost-benefit analysis of Aadhaar" dated 09.11.2012 has made the following findings:-

- i. A key problem with the implementation of MNREGS is diversion of funds, through ghost beneficiaries and inflated/ fake work records. Based on data collected from 8 states ,... found a great deal of fraud such as making of **fake job cards** and improper maintenance of muster rolls.
- ii. Using the data from these various surveys, we estimate **that a leakage of approximately 12 percent is being caused to the government on account of ghost workers and manipulated muster rolls**. We assume that 5 percent of the leakages can be plugged through wage disbursement using Aadhaar-enabled bank accounts and 7 percent through automation of muster rolls. [Page 25 r/w 428 of CAA]
- iii. The government has to face losses in the form of wasteful expenditure and leakages arising due to inflated enrolment data. Aadhaar can help address this concern by providing a robust tracking mechanism to monitor the enrolment and attendance of students. On the one hand this will help address the problem of inflated enrolments of fictitious students and on the other, it will allow for real-time monitoring of the benefit distributions using attendance records. Any unused resources available with the school due to student absenteeism can be therefore be adjusted by the central government while making subsequent allocations to the state. In addition, the use of Aadhaar in the PDS distribution system will help plug leakage of food grains, which are to be disbursed to schools through the Food Stamp Programme (FSP). We assume that the integration of Aadhaar with the MDM scheme in the manner contemplated above will enable the government to save approximately 10 percent of the costs that it currently incurs on the scheme. [Page 25 r/w 429 of CAA]
- iv. Leakages also exist in the distribution of books, scholarships, uniforms and bicycles to students under education schemes, which can be addressed by linking the distribution of these benefits with Aadhaar. [Page 26 r/w 430 of CAA]

39. The Economic Survey 2015-16 at Chapter 3 titled “Spreading JAM Across India’s economy” observed as follows:-

- i. To identify beneficiaries, the government needs databases of eligible individuals. Beneficiary databases have existed for long before Aadhaar, but their accuracy and legitimacy have been hampered by the administrative and political discretion involved in granting identity proofs like BPL cards, driving licenses and voter IDs. **Ghost and duplicate names crept into beneficiary lists, leading to leakage.** Aadhaar’s virtue lies in using technology to replace human discretion, while keeping the system simple enough – fingerprints and iris scans – for citizens to understand. [Page 29 r/w 467 (Vol-II) of CAA]
- ii. JAM significantly reduced leakages in LPG and MGNREGS with limited exclusion of the poor. [Page 29 r/w 467 (Vol-II) of CAA]
- iii. **With DBT in place, the government identifies beneficiaries by linking households’ LPG customer numbers with Aadhaar numbers to eliminate ‘ghost’ and duplicate households from beneficiary rolls.** [P. 461 of Vol-II – CAA]

40. The Economic Survey 2014-15 at Chapter 3 titled “Wiping Every Tear from every Eye: The JAM Number Trinity Solution” dated February, 2015 analyses the possibilities offered by the JAM Trinity – Jan Dhan, Aadhaar, Mobile to effectively target public resources to those who need it most.

- i. Data show that only 59 percent of subsidized kerosene allocated via the PDS is actually consumed by households, with the remainder lost to leakage and only 46 percent of total consumption is by poor households. [Page 31 r/w 486 (Vol-II) of CAA]
- ii. Even in the case of the food distributed via the PDS, leakages are very high (about 15 percent for rice and 54 percent for wheat). [Page 31 r/w 486 (Vol-II) of CAA]
- iii. A recent study reported evidence from Andhra Pradesh where MGNREGA and social security payments were paid through

Aadhaar-linked bank accounts. Households received payments faster with the new Aadhaar linked DBT system, and leakages decreased so much that the value of the fiscal savings – due to reduced leakages – were 8 times greater than the cost of implementing the program. **Much of the leakage reduction resulting from biometric identification stems from fewer ghost beneficiaries.** Indeed, the government is already realizing the gains from direct benefit transfers areas by paying cooking gas subsidies directly into the bank accounts of 9.75 Crore recipients. [Page 32 r/w 486 (Vol-II) of CAA]

41. The United Nations in its report titled, “Leaving No One Behind: the imperative of inclusive development” praises India’s decision of launching the Aadhaar Programme:-
 - i. The decision of India in 2010 to launch the Aadhaar programme to enroll the biometric identifying data of all its 1.2 billion citizens, for example, was a critical step in enabling fairer access of the people to government benefits and services. Programme such as Aadhaar have tremendous potential to foster inclusion by giving all people, including the poorest and the most marginalized an official identity. Fair and robust systems of legal identity and birth registration are recognized in the new 2030 Agenda for Sustainable Development as an important foundation for promoting inclusive societies. [Page 33 r/w 516 (Vol-II) of CAA]
42. The Centre for Global Development published Policy Paper No. 114 dated December, 2017 titled “Fuel Subsidy Reform in Developing Countries: Direct Benefit Transfer of LPG Cooking Gas Subsidy in India.” dated December, 2017 highlighting the importance of Aadhaar in the process of direct benefit transfers and how other alternatives like Smart Cards etc had failed to achieve the desired objective:

- i. India's LPG reform is a rare case of success in achieving reform in the difficult area of energy subsidy reform. [Page 34 r/w 538 (Vol-II) of CAA]
- ii. PaHaL has increased efficiency and reduced leakages compared to the previous in-kind subsidy regime, resulting in significant fiscal savings for the government at fraction of the cost of the program. [Page 34 r/w 538 (Vol-II) of CAA]
- iii. The reform program in India adopted a two-pronged approach. On the one hand, it has cleaned up and pruned the subsidy beneficiary lists. This involved the one-time removal of duplicate and ghost connections through a Know Your Customer (KYC), which reduced diversion of subsidized LPG cylinders from domestic to commercial use using these ghost connections. The KYC process also prevents duplicate enrollments in the 10-12 million new customers who apply for LPG connections each year. The program also allowed the move to target subsidies that were previously universal. . [Page 35 r/w 539 (Vol-II) of CAA]
- iv. By putting in place a system of standardized, **deduplicated** list of consumers, the program will improve the targeting and distribution of public resources on fuel subsidies for the foreseeable future. . [Page 35 r/w 539 (Vol-II) of CAA]
- v. **To tackle the issue, governments have tried various initiatives—**including color coding LPG cylinders (red for domestic, blue for commercial use), raids on warehouses by criminal investigating agencies and radio frequency (RFID) tagging with smartcards that could track consumers. **However, none of these efforts addressed the core problems effectively i.e. -duplicate/ghost LPG connections.** [Page 35 r/w 540 (Vol-II) of CAA]
- vi. De-duplication continued at a steady pace. By March 2017, the government had cumulatively blocked **35.85 million duplicate/ghost LPG connections** as shown in Table 1. [Page 36 r/w 547 (Vol-II) of CAA]
- vii. Analysis of the rollout indicates that **Aadhaar-based direct subsidy transfer reduced fuel purchases in the domestic sector by more than 11 percent, mainly through a reduction in diversion**

through ghost beneficiary accounts. [Page 36 r/w 553 (Vol-II) of CAA]

43. It is further pertinent to note that the importance and utility of Aadhaar for delivery of public services like PDS, has also been endorsed and directed/recommended by this Hon'ble Court in earlier decisions.
44. This Hon'ble Court in the case of **PUCL Vs. Union of India (2011) 14 SCC 331** has approved the recommendations of the High Powered Committee headed by Justice D.P Wadhwa, which recommended linking of Aadhaar with PDS and encouraged State Governments to adopt the same. [Page 37 r/w 574 (Vol-II) of CAA]

“1. The High-Powered Committee headed by Justice D.P. Wadhwa, Retired Judge of this Court, has submitted a preliminary report on the computerisation of public distribution system. In the recommendations of the report it is mentioned that computerisation of PDS consists of primarily three components i.e. creating and updating beneficiary database, stock management from FCI till FPS and sale of commodities at fair price shops. In order to make PDS effective it is important that the delivery and management system is transparent. The citizen participation for social audit can play a crucial role in ensuring effectiveness of the system.

2. In order to implement this system across the country, the following actions are suggested by the Committee:

1. End-to-end computerisation of PDS may be considered in two parts and following prioritisation of the implementation strategy may be followed:

Component I: Diversions, leakages, delays in allocation and transportation, inappropriate distribution of foodgrains to fair price shops go unchecked because of lack of visibility of this information in the public domain.

Computerisation of complete supply chain management up to the shop level and

availability of this information on a transparency portal in public domain is to be accorded the highest priority. The portal should have different dashboards catering to the information needs of all the stakeholders.

Component II: Electronic authentication of delivery and payments at the fair price shop level. In order to ensure that each cardholder is getting his due entitlement, computerisation has to reach literally every doorstep and this could take long. Moreover, several States have already started implementing smart cards, food coupons, etc. which have not been entirely successful. **Reengineering these legacy systems and replacing it with the online Aadhaar authentication at the time of foodgrain delivery will take time. This is therefore proposed as Component II.**

2. The Department of Food and Public Distribution is directed to immediately issue guidelines to all the States for end-to-end computerisation of TPDS.

3. The Government of India shall ensure that the State Governments prepare a time-bound action plan for completing the process of computerisation. This action plan will be implemented keeping the timelines in mind and will be regularly submitted before the Hon'ble Supreme Court.

4. The States/UTs should take up end-to-end computerisation of TPDS as a top priority and should appoint a dedicated nodal officer to monitor the projects related to TPDS computerisation.

5. **The States/UTs may be encouraged to include the PDS related KYR+ field in the data collection exercise being undertaken by various Registrars across the country as part of the UID (Aadhaar) enrolment.**

6. Digitisation of beneficiary data and a centralised database with clear process of data updation to be put in place by the States in a time-bound manner.

....

10. As the process of end-to-end computerisation is expected to be a sizable exercise, to complete it in a mission mode, a separate and dedicated institutional mechanism is to be incorporated to look after the progress of computerisation of PDS. This institution must have active participation of all stake-holders including the State Governments. As PDS is implemented by the State by the State Governments and supported by the Government of India, role of the State Government in this body will be helpful in getting required support from the State Governments.

...

12. As far as possible, the State Governments should be directed to link the process of computerisation of Component 2 with Aadhar registration. This will help in streamlining the process of biometric collection as well as authentication. The States/UTs may be encouraged to include the PDS related KYR+ field in the data collection exercise being undertaken by various Registrars across the country as part of the UID (Aadhar) enrolment.”

45. The Supreme Court of India, while monitoring the PILs relating to night shelters for the homeless and the right to food through the public distribution system, has lauded and complemented the efforts of State Governments for *inter alia* carrying out biometric identification of the head of family of each household to eliminate fictitious, bogus and

ineligible BPL/AAY household cards. This is evident from the following extracts in **PUCL v. Union of India (2010) 13 SCC 45** :

“48. In the affidavit, it is mentioned that NGO, Samya had conducted survey and identified 15,000 homeless beneficiaries of which 14,850 which have been approved for giving “homeless cards”. **These cards are being prepared zone wise and the list is displayed at the office of the Assistant Commissioners/Circle Office for distribution of the special homeless cards to the beneficiaries after obtaining their biometric impressions.** The NGO, Samya has also been informed to facilitate delivery of these cards to the beneficiaries and enable them to lift the specified food articles and kerosene oil allocated from the linked fair price shop/kerosene oil depot. The details have been mentioned in the AAY programme. [Page 37 r/w 593 (Vol-II) of CAA]

49. It is mentioned in the affidavit that under the Central Scheme of Food and Supplies Department, Government of NCT of Delhi is carrying out review of BPL/AAY household cards which were issued before 15-1-2009. **It is simultaneously carrying out biometric identification of head of family of each household to eliminate fictitious, bogus and ineligible cards and those who have left Delhi.** [Page 38 r/w 593 (Vol-II) of CAA]

....

53. The Delhi Government has very minutely and carefully analysed the problems of homeless people living in these shelters and is trying to provide a comprehensive programme for the homeless. We must compliment the Government of NCT of Delhi for this effort. [Page 38 r/w 594 (Vol-II) of CAA]”

46. Similarly, a Division bench of this Hon’ble Court in **PUCL (PDS matters) v. Union of India & Ors. (2013) 14 SCC 368** has held that computerisation is going to help the public distribution system in the country in a big way and encouraged and endorsed the digitization of database including biometric identification of the beneficiaries. In fact the Supreme Court had requested Mr. Nandan Nilekani, the then Chairman, UIDAI to suggest ways in which the computerisation

process of PDS can be expedited. The following extracts from the abovementioned order is relied upon:

[Page 38 r/w Pg. 598 (Vol-II) of CAA]

“2. There seems to be a general consensus that computerisation is going to help the public distribution system in the country in a big way. In the affidavit it is stated that the Department of Food and Public Distribution has been pursuing the States to undertake special drive to eliminate bogus/duplicate ration cards and as a result, 209.55 Lakh ration cards have been eliminated since 2006 and the annual saving of foodgrains subsidy has worked out to about Rs 8200 crores per annum. It is further mentioned in the affidavit that end-to-end computerisation of public distribution system comprises creation and **management of digitised beneficiary database including biometric identification of the beneficiaries**, supply chain management of TPDS commodities till fair price shops.

3. It is further stated in the affidavit that in the State of Gujarat, the process of computerisation is at an advanced stage where issue of bar coded ration cards has led to a reduction of 16 Lakh ration cards. It is expected that once the biometric details are collected, this number would increase further. For the present, a reduction of 16 Lakh ration cards would translate into an annual saving of over Rs 600 crores. **This is just to illustrate that computerisation would go in a big way to help the targeted population of the public distribution system in the country.**

4. In the affidavit it is further mentioned that the Government of India has set up a task force under the Chairmanship of Mr. Nandan Nilekani, Chairman, UIDAI, to recommend, amongst others, an IT strategy for the public distribution system. We request Mr Nandan Nilekani to suggest us ways and means by which computerisation process of the public distribution system can be expedited. Let a brief report/affidavit be filed by Mr Nandan Nilekani within four weeks from today.”

47. Section 12 of the National Food Security Act 2013 also envisages use of Aadhaar for unique identification and proper targeting of benefits:

“REFORMS IN TARGETED PUBLIC DISTRIBUTION SYSTEM

12. (1) The Central and State Governments shall endeavour to progressively undertake necessary reforms in the Targeted Public Distribution System in consonance with the role envisaged for them in this Act.

(2) The reforms shall, inter alia, include—

doorstep delivery of foodgrains to the Targeted Public Distribution System outlets;

application of information and communication technology tools including end-to-end computerisation in order to ensure transparent recording of transactions at all levels, and to prevent diversion;

leveraging "aadhaar" for unique identification, with biometric information of entitled beneficiaries for proper targeting of benefits under this Act; . . .”

48. It is also important to advert to the judgment of this Hon’ble Court in *Binoy Viswam v. Union of India* 2017 (7) SCC 59 which has also rendered its findings on the objectives of Aadhaar, while examining the reasonable nexus of the law with the object sought to be achieved, which would be directly applicable to the present case as well. The relevant extract reads as follows-

“125. By making use of the technology, a method is sought to be devised, in the form of Aadhaar, whereby identity of a person is ascertained in a flawless manner without giving any leeway to any individual to resort to dubious practices of showing multiple identities or fictitious identities. That is why it is given the nomenclature “unique identity”. It is aimed at securing advantages on different levels some of which are described, in brief, below:

125.1. In the first instance, as a welfare and democratic State, it becomes the duty of any responsible Government to come out with welfare schemes for the upliftment of poverty-stricken and marginalised sections of the society. This is even the ethos of Indian Constitution which casts a duty on the State, in the form of “directive principles of State policy”, to take adequate and effective steps for betterment of such underprivileged classes. State is bound to take adequate measures to provide education, health care, employment and

even cultural opportunities and social standing to these deprived and underprivileged classes. It is not that Government has not taken steps in this direction from time to time. At the same time, however, harsh reality is that benefits of these schemes have not reached those persons for whom that are actually meant.

125.1.1. India has achieved significant economic growth since Independence. In particular, rapid economic growth has been achieved in the last 25 years, after the country adopted the policy of liberalisation and entered the era of, what is known as, globalisation. Economic growth in the last decade has been phenomenal and for many years, the Indian economy grew at highest rate in the world. At the same time, it is also a fact that in spite of significant political and economic success which has proved to be sound and sustainable, the benefits thereof have not percolated down to the poor and the poorest. In fact, such benefits are reaped primarily by rich and upper middle classes, resulting into widening the gap between the rich and the poor.

125.1.2. Jean Dreze and Amartya Sen pithily narrate the position as under [*An Uncertain Glory : India and its Contradictions*] :

“Since India's recent record of fast economic growth is often celebrated, with good reason, it is extremely important to point to the fact that the societal reach of economic progress in India has been remarkably limited. It is not only that the income distribution has been getting more unequal in recent years (a characteristic that India shares with China), but also that the rapid rise in real wages in China from which the working classes have benefited greatly is not matched at all by India's relatively stagnant real wages. No less importantly, the public revenue generated by rapid economic growth has not been used to expand the social and physical infrastructure in a determined and well-planned way (in this India is left far behind by China). There is also a continued lack of essential social services (from schooling and health care to the provision of safe water and drainage) for a huge part of the population. As we will presently discuss, while India has been overtaking other countries in the progress of its real income, it has been overtaken in terms of social indicators by many of these countries, even within the region of South Asia itself (we go into this question more fully in Chapter 3, ‘India in Comparative Perspective’).

To point to just one contrast, even though India has significantly caught up with China in terms of GDP growth, its progress has been very much slower than China's in indicators such as longevity, literacy, child undernourishment and maternal mortality. In South Asia itself, the much poorer economy of Bangladesh has caught up with and overtaken India in terms of many social indicators (including life expectancy, immunisation of children, infant mortality, child undernourishment and girls' schooling). Even Nepal has been catching up, to the extent that it now has many social indicators similar to India's, in spite of its per capita GDP being just about one third. Whereas twenty years ago India generally had the second best social indicators among the six South Asian countries (India, Pakistan, Bangladesh, Sri Lanka, Nepal and Bhutan), it now looks second worst (ahead only of problem-ridden Pakistan). India has been climbing up the ladder of per capita income while slipping down the slope of social indicators."

125.1.3. It is in this context that not only sustainable development is needed which takes care of integrating growth and development, thereby ensuring that the benefit of economic growth is reaped by every citizen of this country, it also becomes the duty of the Government in a welfare State to come out with various welfare schemes which not only take care of immediate needs of the deprived class but also ensure that adequate opportunities are provided to such persons to enable them to make their lives better, economically as well as socially. As mentioned above, various welfare schemes are, in fact, devised and floated from time to time by the Government, keeping aside substantial amount of money earmarked for spending on socially and economically backward classes. However, for various reasons including corruption, actual benefit does not reach those who are supposed to receive such benefits. One of the main reasons is failure to identify these persons for lack of means by which identity could be established of such genuine needy class. Resultantly, lots of ghosts and duplicate beneficiaries are able to take undue and impermissible benefits. A former Prime Minister of this country [Late Shri Rajiv Gandhi] has gone on record to say that out of one rupee spent by the Government for welfare of the downtrodden, only 15 paise thereof actually reaches those persons for whom it is meant. It cannot be doubted that with UID/Aadhaar much of the malaise in this field can be taken care of.

125.2. Menace of corruption and black money has reached alarming proportion in this country. It is eating into the economic progress which the country is otherwise achieving. It is not necessary to go into the various reasons for this menace. However, it would be pertinent to comment that even as per the observations of the Special Investigation Team (SIT) on black money headed by Justice M.B. Shah, one of the reasons is that persons have the option to quote their PAN or UID or passport number or driving licence or any other proof of identity while entering into financial/business transactions. Because of this multiple methods of giving proofs of identity, there is no mechanism/system at present to collect the data available with each of the independent proofs of ID. For this reason, even SIT suggested that these databases be interconnected. To the same effect is the recommendation of the Committee headed by Chairman, CBDT on measures to tackle black money in India and abroad which also discusses the problem of money laundering being done to evade taxes under the garb of shell companies by the persons who hold multiple bogus PAN numbers under different names or variations of their names. **That can be possible if one uniform proof of identity, namely, UID is adopted. It may go a long way to check and minimise the said malaise.**

125.3. **Thirdly, Aadhaar or UID, which has come to be known as the most advanced and sophisticated infrastructure,** may facilitate law-enforcement agencies to take care of problem of terrorism to some extent and may also be helpful in checking the crime and also help investigating agencies in cracking the crimes. No doubt, going by the aforesaid, and may be some other similarly valid considerations, it is the intention of the Government to give fillip to Aadhaar movement and encourage the people of this country to enrol themselves under the Aadhaar Scheme.

126. Whether such a scheme should remain voluntary or it can be made mandatory imposing compulsiveness on the people to be covered by Aadhaar is a different question which shall be addressed at the appropriate stage. **At this juncture, it is only emphasised that mala fides cannot be attributed to this scheme.** In any case, we are concerned with the vires of Section 139-AA of the Income Tax Act, 1961 which is a statutory provision. This Court is, thus, dealing with the

aspect of judicial review of legislation. Insofar as this provision is concerned, the explanation of the respondents in the counter-affidavit, which has already been reproduced above, is that the primary purpose of introducing this provision was to take care of the problem of multiple PAN cards obtained in fictitious names. Such multiple cards in fictitious names are obtained with the motive of indulging into money laundering, tax evasion, creation and channelising of black money. It is mentioned that in de-duplication exercises, 11.35 Lakh cases of duplicate PANs/fraudulent PANs have been detected. Out of these, around 10.52 lakhs pertain to the individual assesseees. **Parliament in its wisdom thought that one PAN to one person can be ensured by adopting Aadhaar for allotment of PAN to individuals. As of today, that is the only method available i.e. by seeding of existing PAN with Aadhaar. It is perceived as the best method, and the only robust method of de-duplication of PAN database.** It is claimed by the respondents that the instance of duplicate Aadhaar is almost non-existent. It is also claimed that seeding of PAN with Aadhaar may contribute to widening of the tax case as well, by checking the tax evasions and bringing into tax hold those persons who are liable to pay tax but deliberately avoid doing so.

129. The respondents have also claimed that linking of Aadhaar with PAN is consistent with India's international obligations and goals. In this behalf, it is pointed out that India has signed the Inter-Governmental Agreement (IGA) with USA on 9-7-2015, for Improving International Tax Compliance and implementing the Foreign Account Tax Compliance Act (FATCA). India has also signed a multilateral agreement on 3-6-2015, to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters under the Common Reporting Scheme (CRS), formally referred to as the Standard for Automatic Exchange of Financial Account Information (AEOI). As part of India's commitment under FATCA and CRS, financial sector entities capture the details about the customers using the PAN. In case the PAN or submitted details are found to be incorrect or fictitious, it will create major embarrassment for the country. Under Non-filers Monitoring System (NMS), the Income Tax Department identifies non-filers with potential tax liabilities. Data analysis is carried out to identify non-filers about whom specific information was available in AIR, CIB data and

TDS/TCS returns. Email/SMS and letters are sent to the identified non-filers communicating the information summary and seeking to know the submission details of income tax return. In a large number of cases (more than 10 Lakh PANs every year) it is seen that the PAN holder neither submits the response and in many cases the letters are return unserved. Field verification by field formations have found that in a large number of cases, the PAN holder is untraceable. In many cases, the PAN holder mentions that the transaction does not relate to them. **There is a need to strengthen PAN by linking it with Aadhaar/biometric information to prevent use of wrong PAN for high value transactions.**

130. While considering the aforesaid submission of the petitioners, one has to keep in mind the aforesaid purpose of the impugned provision and what it seeks to achieve. The provision is aimed at seeding Aadhaar with PAN. We have already held, while considering the submission based on Article 14 of the Constitution, that the provision is based on reasonable classification and that has nexus with the objective sought to be achieved. **One of the main objectives is to de-duplicate PAN cards and to bring a situation where one person is not having more than one PAN card or a person is not able to get PAN cards in assumed/fictitious names. In such a scenario, if those persons who violate Section 139-AA of the Act without any consequence, the provision shall be rendered toothless. It is the prerogative of the legislature to make penal provisions for violation of any law made by it. In the instant case, requirement of giving Aadhaar enrolment number to the designated authority or stating this number in the income tax returns is directly connected with the issue of duplicate/fake PANs.**

49. In light of the above submissions, the state's legitimate interest and a compelling need of introducing Aadhaar for identification of genuine beneficiaries of subsidies, services and benefits under the Aadhaar Act or elimination of fake PAN Cards, has been upheld by a Constitution Bench of the Supreme Court while also holding that the Act does not create an electronic leash or surveillance state.

50. With reference to Annexure P1 of the writ petition (News report dated 22.06.2017), it is submitted that the role of UIDAI is limited to issue of Aadhaar numbers and provide authentication services for establishing identity of the beneficiaries. The usage of Aadhaar for delivery of welfare service, benefits etc. or for any other purpose authorized by law and the extent to which Aadhaar is to be used is to be determined by the Implementing Agencies such as State Governments/Central Ministries and other authorities etc. The UIDAI does not define the nature of benefits and services that should be or can be delivered. It is for the State Governments/Ministries/Departments to decide whether delivery of the benefits and services should be linked to Aadhaar number and the extent to which the number should be used. The Hon'ble Supreme Court in Aadhaar judgment has stated that 'Benefits' and 'services' as mentioned in Section 7 should be those which have the colour of some kind of subsidies etc., namely, welfare schemes of the Government whereby Government is doling out such benefits which are targeted at a particular deprived class. It would cover only those 'benefits' etc. the expenditure thereof has to be drawn from the Consolidated Fund of India.
51. Moreover, the Hon'ble Supreme Court has struck down the PMLA Rules relating to mandatory linking of Aadhaar with Bank Accounts in the present form and the Circular dated March 23, 2017 mandating linking of mobile number with Aadhaar has also been quashed. Therefore, the grievance of the Petitioner regarding mandatory linking of his Aadhaar number to his bank account or mobile number has already been redressed in the Aadhaar judgment.

52. The Hon'ble Court has further held that portion of Section 57 of the Aadhaar Act which enables body corporate and individuals to seek authentication to be unconstitutional.

Apprehensions Regarding Security of Aadhaar Data-

53. Further, on the aspect of Security of Aadhaar Data, the apprehensions raised in the present writ petition, stand assuaged with the striking down or reading down or clarification of some of the provisions by the Hon'ble Supreme Court:

- (i) Authentication records are not to be kept beyond a period of six months, as stipulated in Regulation 27(1) of the Authentication Regulations. This provision which permits records to be archived for a period of five years is held to be bad in law.
- (ii) Metadata relating to transaction, as provided in Regulation 26 of the aforesaid Regulations in the present form, held to be impermissible.
- (iii) Section 33(1) of the Aadhaar Act read down by clarifying that an individual, whose information is sought to be released, shall be afforded an opportunity of hearing.
- (iv) Section 33(2) of the Act in the present form is struck down.
- (v) That portion of Section 57 of the Aadhaar Act which enables body corporate and individual to seek authentication held to be unconstitutional.
- (vi) Respondents directed to bring out a robust data protection regime in the form of an enactment on the basis of Justice B.N. Srikrishna (Retd.) Committee Report with necessary modifications thereto as may be deemed appropriate.

54. It is submitted that the petitioners submission in Para 16(ii) that demographic information which he has parted with like his name, residential address, date of birth, email address and mobile number which is his valuable personal and private information has been compromised is completely devoid of any substance or truth and the petitioner may be put to the strictest proof to show how any personal information pertaining to the petitioner has been compromised or rendered insecure in any manner whatsoever. Moreover the Supreme Court in the Aadhaar judgement has held that there is no reasonable expectation of privacy in minimal data collected by way of demographic information which is already freely available. Reliance is placed on Para 193 of the majority judgment in *Puttaswamy* which reads as follows:

“193. Demographic information, both mandatory and optional, and photographs does not raise a reasonable expectation of privacy under article 21 unless under special circumstances such as juveniles in conflict of law or a rape victim’s identity.”

55. It is further submitted that the contents of the petition contained in para 16(iii) have been rendered infructuous in light of the judgement of the Supreme Court. The Supreme Court has upheld the linking of Aadhaar with PAN as well as for filing income tax returns and this was recently reiterated by the order of the honourable Supreme Court dated 04.02.2019 in *Union of India v. Shreya Sen* arising out of SLP(C) Diary No. 34292/2018 wherein it was categorically held as follows:

“Thereafter, this court has decided the matter and upheld the vires of section 139AA of the Income Tax Act. In view thereof, linking of PAN with Aadhaar is mandatory”

True Copy of the Order dated 04.02.2019 of Hon’ble Supreme Court is marked as **Annexure R - 8**

56. As stated above, Petitioner has based the entire writ petition on the alleged data breach reported in certain sections of media. The answering Respondent vehemently denies such false and baseless allegations and humbly submits that there has been no security breach of UIDAI’s biometric database or Central Identity Data Repository (CIDR). It is quite curious that reading of press reports without actual verification of its impact on the petitioner affected his privacy, personhood and dignity and the petitioner felt so distressed without even verifying as to whether his data was at all compromised. It is strongly denied that any data breach has occurred in the CIDR or that the petitioners right has been affected in any manner whatsoever. The petitioner has not been able to demonstrate how his rights have been affected.
57. It is respectfully submitted that the existing security controls and protocols of Respondent No.1 are robust and capable of countering any such attempts or malicious designs of data breach or hacking. Security of Aadhaar is of critical importance and is given paramount significance by the Respondent. Respondent No.1 constantly strengthens and reviews its infrastructure and ecosystems in line with the best international security practices and technological standards and has multi-layered security and privacy considerations built into the core

strategy of Aadhaar with three basic doctrines of minimal information, optimal ignorance and federated database which give higher level of security to the data.

58. Moreover, various policies and procedures for securing the data have been defined and are reviewed and updated continually by the answering Respondent for controlling and monitoring any movement of people, material and data in and out of its secured and well-guarded premises, particularly the data centres.
59. It is therefore stated at the cost of repetition that the data is fully secured/ encrypted at all the times i.e. at rest, in transit and in storage. For, further strengthening of security and privacy of data, security audits are conducted on regular basis, and all possible steps are taken to make the data safer and protected. Further, there are multiple layers of security at physical level in UIDAI Data Centres and is being managed by armed CISF personnel round the clock. Strengthening of security of data is an ongoing process and all possible steps are being taken in this regard.
60. The security assurance of Aadhaar ecosystem has further been strengthened manifold with the enactment of The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits And Services) Act, 2016 which has stringent penalties/ punishments for any such breach of security.
61. Insofar as the use and protection of data is concerned, having regard to the principles enshrined in various case laws, both Indian and foreign, the matter is examined from the stand point of data minimisation, purpose limitation, time period for data retention, data protection and

security (qua CIDR, requisite entities, enrolment agencies and Registrars, authentication service agency, hacking, biometric solution providers, substantive procedural and judicial safeguards).

62. Before proceeding to advert to the specific submissions of the petitioner it would be appropriate to place before this Hon'ble court the entire security measures including the legislative and technological measures in place to ensure safe guard of security of data collected by the Unique Identification Authority Of India.

DATA SECURITY IN AADHAAR

63. **Legislative Safeguards on Data Security:** Chapter VI of the Aadhaar Act, 2016 deals with protection of information. Section 28 of the Act pertains to security and confidentiality of the information wherein the Authority is statutorily required to ensure the security of identity information and authentication records of individuals including information stored in the Central Identity Data Repository and the same must be secured and protected against access, use or disclosure not permitted under the Act and against accidental or intentional destruction, loss or damage. The Authority is also statutorily required to ensure that the agencies, consultants, advisors or other persons appointed or engaged for performing any function of the Authority under this Act, have in place appropriate technical and organizational security measures for the information.
64. There is also a prohibition against the Authority or its officers, serving or retired, from revealing any information stored in the Central Identities Data Repository or authentication record to anyone except to

the Aadhaar number holder who may request the Authority access to his own identity information excluding his core bio-metric information.

65. Chapter VII of the Act contains provisions relating to offences and penalties inter alia relating to impersonation, identity theft, unauthorized use, transmission or collection of identity information, unauthorized access to CIDR, etc. which are punishable with imprisonment upto 3 years and/or with fine.

66. This Hon'ble Court's attention may also be drawn to Aadhaar (Data Security) Regulations, 2016 which was notified on 12.09.2016 and came into force on 14.09.2016. The relevant security obligations on various stakeholders under the subordinate legislation are provided therein. Therefore, the Petitioner's allegations that involvement of private entities in the process of enrolment etc would compromise the security of data is misplaced as any entity involved in the process are subject to stringent controls both technologically as well as under the law. Nevertheless, a policy decision has been taken that the Enrolments will be done under the supervision and control of State Govt, Banks and Post Offices will conduct Aadhaar enrolments.

True Copy of the Decision of the Government dated 29.09.2017 is marked as **Annexure R -9**

67. It is also pertinent to state that the UIDAI's Central Identities Data Repository (CIDR) in which the data is stored has been declared as

“Protected System” under Section 70 of the Information Technology Act, 2000 whereby the government can declare any computer resource, which directly or indirectly affects the facility of critical information infrastructure to be a protected system. The Explanation to Sec. 70 defines Critical Information Infrastructure to mean the computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety. Section 70 (3) states that any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment upto 10 years and will also be liable to fine. Therefore, by declaring the UIDAI and CIDR as critical information infrastructure the Government has underlined its emphasis on security and further bolstered the security regime surrounding Aadhaar wherein any breach will be met with the strictest punishment provided for under the law. Therefore, the Petitioner’s argument that Aadhaar is an insecure technology project is specious and devoid of any substance.

True Copy of the notification dated 11.12.2015 issued by Ministry of Communication & Information Technology is annexed herewith and is marked as **Annexure –R –10**

68. There are various measures under the Aadhaar Act, 2016 and Aadhaar (Authentication) Regulations and other regulations to ensure that AUAs do not store biometric and that they are compliant with the requirements. These are as follows.

69. Section 8 (2) of the Aadhaar Act, 2016 mandates that the Identity information shall only be used for submission to Central Identities Data Repository for authentication.
70. Section 29 (1) & Section 29 (2) of the Aadhaar Act, 2016 prohibit sharing of biometric information and use of biometric information other than for generation of Aadhaar number generation and authentication.
71. Section 37 of the Aadhaar Act, 2016 prohibits disclosure, transmission, copying or other dissemination of any identity information to a person not authorized under the Act or regulations makes it an offence punishable with imprisonment which may extend to 3 years and/or fine upto 1 lakh rupees.
72. Regulation 17(1)(a) of the Aadhaar (Authentication) Regulations, 2016 specifically prohibits a requesting entity from storing, sharing or publishing for any reason whatsoever any core biometric information collected from the Aadhaar number holder and also prohibits retention of any copy of the core biometric information.
73. Regulation 7(1), 7(2), 9(1), 9(5), 17 (1) (a) (b) (c) (d) (e) of Aadhaar (Authentication) Regulations mandate AUAs to secure biometric information and state how the application should process biometric information and measures against storage of biometric information.
74. Regulation 11 of Aadhaar (Authentication) Regulations provides a facility wherein residents can lock their biometrics as a further safeguard against misuse.

75. Regulation number 14 (1) (h) of Aadhaar (Authentication) Regulations mandate yearly audit of AUA operations and systems by information systems auditor certified by a recognized body.
76. Notice was issued by UIDAI dated 28-Feb-2017 reinforcing that biometrics should not be stored and replayed by AUAs and mandating AUAs to submit an audit compliance certificate.
77. **Technological Safeguards on Data Security in Aadhaar:-**It is submitted that the technical architecture of Aadhaar has been structured in such a way, so as to ensure clear data verification, authentication and de-duplication, while ensuring a high level of privacy and information security. The collection of minimal biometric data and fully secure end to end encryption, as well as logical partitioning, firewalling and anonymisation of decrypted biometric data protects the privacy of individuals as also prevents tampering of biometric information.
78. It is submitted that the UIDAI has taken all necessary safeguards, starting from providing standardized software that encrypts the entire data even before saving it to any disk, protecting data using tamper proofing, identifying every operator in all and every enrolment, identifying every one of the thousands of machines using a unique machine registration process, which ensures every encrypted data is tracked.
79. The data collection software, termed as the Enrolment Client, is created and managed centrally by the UIDAI. Any user of the client needs to authenticate each enrolment with a biometric sign off, which is a highly

secure confirmation. The biometric information is encrypted and only then is it stored. Hence the operator has no access to this information. The encryption system follows a private key/public model. The private key is available only with UIDAI at the processing location called the Central Identities Data Repository (CIDR). Hence, even if data packets are lost or stolen, the biometric information regarding the same cannot be accessed and hence cannot be misused.

80. The biometrics available with UIDAI are not shared with anyone. Only a 'Yes/No' response is given at the time of biometric authentication of the person. UIDAI has an active data security policy that addresses all aspect of data collection, data handling and data storage. It is denied that the biometric information used can be accessed or used without any protection to the individual or that it can fall in the hands of foreign Governments. The security and integrity of the data has been enshrined in the Strategy.
81. Further, there is no question of facilitating any access to personal data of residents. Data access is only given when due authorisation is provided by the resident. The minimal demographic data which is collected under Aadhaar in respect of enrolees is actually already available with several agencies in the country and some of it is also available in various public domains (For e.g. in the form of electoral rolls, PAN card, telephone directories etc.).
82. It is submitted that that UIDAI has taken fool-proof measures to ensure end-to-end security of resident data, spanning from full encryption of resident data at the time of capture, tamper resistance, physical security, access control, network security, stringent audit mechanism,

24x7 monitoring, and measures such as data partitioning and data encryption within UIDAI controlled data centres. In particular, at the enrolment centres and field operations level, the following safeguards have been implemented.

102.1 Standard enrolment software for all its registrars, to ensure uniformity of enrolment data capture and processes.

102.2 All operators / supervisors are required to be trained themselves and certified as operator / supervisor before they can start enrolling.

102.3 Every enrolment packet is biometrically signed by the operator ensuring traceability and non-repudiation. As a result the authenticity of one's signature cannot be denied.

102.4 Every packet is reviewed by a supervisor for data quality (review audits are captured electronically) and signed as required which means every enrolment is traceable in terms of "who", "when", "where", "under which agency", "under which registrar", "who reviewed it", etc.

102.5 Data collected during enrolment using UIDAI provided software ensures that the resident data including raw biometrics is encrypted using strong asymmetric encryption technologies before even saving to disk. It is to be noted that raw biometrics is NEVER stored anywhere without encryption.

102.6 The enrolment software uses standard, best in class, cryptographic techniques while storing resident data on field enrolment stations. It uses, encryption based on PKI (which is an asymmetric public/private key encryption scheme) which

means that no one can decrypt and misuse the data, even if they are in possession of the enrolment packet.

102.7 During transit of the data from enrolment stations on the field to UIDAI data centres, the following steps are ensured (a) every enrolment data packet is "always" stored in PKI encrypted, tamper proof files and is never decrypted or modified during transit; (b) the enrolment data is never decrypted until it reaches UIDAI's data centres secure production zone.

83. It is submitted that the strong asymmetric encryption technologies used to encrypt every resident's data packet ensures that no agency or person can access, modify, or misuse the resident data during field enrolment or in transit to the UIDAI data centre. The encryption technology used is 2048 bit encryption which is the strongest available encryption and it is impossible to decrypt and extract any information even if enrolment packets are accessible during transit to UIDAI data centre.
84. At the time of enrolment, resident's demographic data along with ten fingerprint, two iris and photo of the face is captured. For generation of Aadhaar number, fingerprint and iris data is matched (1:N) against all the data available in CIDR. Subsequently, template of fingerprint and iris are generated in ISO format and the same along with demographic data and photo is stored securely in UIDAI authentication server database.
85. The Aadhaar authentication is performed through multi-layered channels of trusted partners viz. Authentication Service Agencies (ASAs) and Authentication User Agencies (AUAs) having secured leased line connectivity. These partners, having signed Agreements

with UIDAI, are bound to comply with the provisions of Aadhaar Act, 2016, its Regulations, Agreement, specifications, standards, technical architecture and guidelines issued by UIDAI from time to time. All authentication related data to and from UIDAI traverse only in an encrypted form using a very high i.e. 2048 bit key asymmetric algorithm.

86. UIDAI has mandated use of Registered Devices (RD) for all authentication requests. With Registered Devices biometric data is signed within the device using the provider key to ensure it is indeed captured live. The device provider RD service forms the encrypted PID block before returning to the host application. This RD service encapsulates the biometric capture, any user experience while capture (such as preview, liveness etc), and signing and encryption of biometrics all within it. Therefore, introduction of RD in Aadhaar authentication system rules out any possibility of storage and replay for biometrics.
87. After collecting the Aadhaar number fingerprint information from the Aadhaar number holder, the client application immediately packages and encrypts these input parameters into PID block before any transmission and send it to UIDAI. At the time of authentication, the Aadhaar number and fingerprint information submitted by an Aadhaar number holder are matched with the biometric information of the said Aadhaar number holder available in the CIDR.
88. Requesting entity shall ensure that the encrypted PID block is not stored, unless it is for buffered authentication where encrypted PID

block may be held temporarily on the authentication device for a short period of time, and that the same is deleted after transmission.

89. Moreover, top experts in the field of Information Technology have also reviewed the entire Aadhaar project and visited the Data Centre in Bangalore with the objective to appraise first-hand the data security measures being implemented. **The Report of the Committee On The Outcome Review of the UID Scheme** submitted by Prof. Rajat Moona, Director, IIT Bhilai Prof. S. Sadagopan, Director, IIIT Bangalore and Prof. Deepak B. Phatak, Dept. of CSE, IIT Bombay have after extensive review found the Aadhaar system to be secure. The said Committee after examination of all facets prepared the report and recommended the continuation of the Aadhaar Project in perpetuity apart from recommending measures to enhance the efficacy and security of the systems. The Committee, inter alia, appreciated the progress of Aadhaar authentication services through its 27 authentication service agencies, 326 authentication user agencies and 255 E-KYC user agencies which have facilitated processing of over 865.05 Crore authentication and 246.96 Crore E-KYC requests by August, 2017. They further observed that UIDAI is processing 2.6 Crore authentication requests per day on a monthly average basis with peak loads at 6 Crore transactions per day. The committee advised UIDAI to prepare for increase in authentication load from 10 Crore per day to 40 Crore per day in the coming months and to 120 Crore per day in a period of next 10 months.

90. The Committee further observed that UIDAI is ISO 27001: 2013 standard compliant that defines security protocols and access protocols to ensure the safety of data. The Committee also observed that UIDAI while providing identity authentication service only informs the requesting agency whether the particular Aadhaar number and the provided biometric is matching or not and that UIDAI only knows that a residence identity is authenticated but it never asks for the purpose and location of such transaction and hence no profiling of the person is possible. Most critically it was observed that the Aadhaar database is not linked with another government/state/private information system.
91. The Committee observed that it is the largest biometric project in the world and that the progress in the project is commendable, touching more than 117 Crore people in a span of 8 years. The Committee also gave the following suggestion/recommendations:
 92. That the technology infrastructure upgradation is most important for UIDAI and that UIDAI must consciously and strategically plan to maintain inventory of active in-service equipment of latest technology.
 93. UIDAI must focus on enhancing its authentication capacity.
 94. The Committee found the need to strengthen the grievance handling mechanism and suggested that UIDAI should set bench marks on grievance resolution timelines and build escalation matrix. Considering the fast changing requirements of Aadhaar and its increased foot prints, Aadhaar grievance handling mechanism will gain importance and hence UIDAI should move towards new automated systems like AI based systems, chatbot etc. for grievance handling.

95. Accordingly the committee recommended the UID scheme to continue beyond the 12th Five Year Plan and that it should be regarded as work in perpetuity in view of its increasing wide-spread use in multiple national activities.

True Copy of the Report of the committee On The Outcome Review of the UID Scheme is marked as **Annexure R –11**

Governance and monitoring measures

96. UIDAI has taken various governance measures to ensure that all AUAs comply with the requirements of various specifications issued by UIDAI through Aadhaar Act 2016, Regulations and other directions issued from time to time.
97. **AUA compliance checklist** from UIDAI includes controls on prevention of biometric / PID block storage for AUAs and controls on securing authentication infrastructure with anti-virus software
98. **AUA Onboarding compliance audit:** Before granting license key to the AUA, every AUA has to submit an audit report against the AUA compliance checklist from a third party auditor
99. **AUA agreement** signed by the AUAs provides measures prohibiting storage of any PID information and ensuring applications are compliant to UIDAI requirement
100. **GRCP** – Service provider of UIDAI has conducted 46 AUA audits on behalf of UIDAI to identify non-compliance with various UIDAI requirements.
101. **Yearly Independent Audits** through CERT-IN empaneled / STQC agencies.

102. **Empanelment of Audit agencies:** UIDAI has initiated empanelment of agencies to conduct audits of AUAs, KUAs and Sub-AUAs.
103. **Empanelment of Agencies for Application certification:** UIDAI has also initiated empanelment of agencies to provide certification of applications used by various AUAs / Authentication ecosystem.

Technical measures

104. **Proactive identification of Replay attacks in CIDR:** Fraud analytics are used in UIDAI to identify replay of biometrics in CIDR. UIDAI conducts a monthly analysis on various AUAs and identifies AUAs replaying stored biometrics. Legal notices are sent periodically to the AUAs which are found to commit any violations.
105. **Biometric locking feature available to resident:** UIDAI provides a facility to the residents to lock their biometrics and prevent misuse of stored biometrics.
106. **API specification documents** of UIDAI guide the AUA organization to secure biometric / PID block at capture.
107. **Trainings Workshops for AUAs** -Periodic workshops are held for AUAs to ensure that they are aware of the security requirements of UIDAI. Last workshops were conducted for the AUAs on 13-June-2017, 14-June-2017, 20-July-2017 and 27-September-2017.

OVERVIEW OF SECURITY REVIEW IN AADHAAR

108. The Aadhaar project is the world's largest national identity project, launched by government of India, which seeks to collect biometric and demographic data of residents and store these in a centralised database. Under the Aadhaar Act 2016, UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of

all stages of Aadhaar life cycle, developing the policy, procedure and system for issuing Aadhaar numbers to individuals and perform authentication and also to ensure the security of identity information and authentication records of individuals.

109. UIDAI-CIDR and associated infrastructure is a Critical Infrastructure and has been declared as Protected System as per Sub-section (1) of Section 70 of IT Act 2000.

110. In reference to Sec 28 (3) of the Aadhaar Act, 2016 vide which UIDAI needs to take necessary measures to secure and protect the information stored in the Central Identities Data Repository (CIDR), UIDAI has taken a number of technical and organizational measures to continuously enhance the security of CIDR and its associated infrastructure.

111. UIDAI endeavours to continuously improve the governance and security of its design, architecture and infrastructure of internal and external ecosystem in order to stay prepared against the continuously evolving sophisticated cyber security attacks and information security threats. The present system of security and governance of UIDAI ecosystem is taken care through following Security Committees whose Roles and Responsibilities are underlined:

112. Security Review Committee was constituted to review and provide advice on Cyber Security matters for UIDAI internal and external ecosystem.

A. Aadhaar - Security Review Committee

- i. UIDAI has established the Security Review Committee to ensure high standards of review, governance and advice on cybersecurity, technology and privacy matters of Aadhaar.
- ii. The Security Review Committee constitutes of well recognized technocrats and professors in the country who are well known for their contributions to the field of Technology and security.

Agenda: The detailed agenda of the Security Review Committee is as follows:

i. Design

- a. Advise on the design of security in UIDAI ecosystem such as secure enrolment, secure authentication, secure printing, biometric processes, network architecture, encryption, and other security in CIDR etc.
- b. Advise on the security aspects in design of critical applications and architecture.
- c. Advise on research and development activities to be undertaken by UIDAI to continuously enhance the design of cyber security in the ecosystem through cyber lab / cyber centre for excellence.
- d. Advise on the resilience of UIDAI operations and disaster recovery measures in response to cyber and physical attacks.
- e. Advise on the security technologies to be deployed by UIDAI to continuously improve the security of the ecosystem.
- f. Advise on proactive and detective fraud management system in the UIDAI ecosystem through appropriate policy and technology measures.

ii. Oversight and Review

- a. Review the threats inherent in the upcoming and existing technology.
- b. Provide strategic inputs on improvement in cyber security through study of major cyber-attack / fraud incidents related to critical infrastructure / National ID programs / privacy in domestic and international arena and identify gaps in the existing cyber security and cyber resilience framework.
- c. Provide inputs on functioning and continuous improvement of the security operations center for UIDAI ecosystem.
- d. Provide inputs the security impact due to significant changes in the solution / design of UIDAI ecosystem.
- e. Provide inputs on any technical security guidelines or standards issued by UIDAI for enhancing security of the ecosystem.
- f. Provide guidance on the response to specific security incidents / events such as ransomware attacks, malware attacks in the country etc.
- g. Provide guidance on the security concerns raised by stakeholders such as NCIIPC, CERT-In, STQC, GRCP, MSP, general public, Parliament, Ministry etc. through various channels such as internal/external assessments, social media, RTI, parliament questions etc.

iii. Governance

- a. Suggest possible policy interventions to strengthen cyber security preparedness of the UIDAI ecosystem.

- b. Advise on the governance measures to be taken to enhance the security of UIDAI ecosystem.
- c. Advise on adoption of security protocols.

iv. Composition

The composition of the Security Review Committee is as follows:

(a) Dr Ajay Bhushan Pandey, CEO, UIDAI	---- Chairman
(b) Dr. Gulshan Rai, NCSC Coordinator	---- Member
(c) Dr. Rajat Moona, Director IIT Bhilai	---- Member
(d) Dr. H Krishnamurthy, Professor, IISc	---- Member
(e) Dr. Manindra Agarwal, Professor, IIT Kanpur	---- Member
(f) Dr. Sandeep Shukla, Professor, IIT Kanpur	----Member
(g) Dr. Subhashis Banerjee, Professor, IIT Delhi	----Member
(h) Dr. S Rakshit, Sc-H, CAIR, DRDO	----Member
(i) Dr. YLP Rao, DDG (Technology), UIDAI	----Convener

True Copy of the qualifications, background and experience of the renowned experts in the Security Review Committee is marked and attached as **Annexure R-12**

B. TARB (Technology and Architecture Review Board) :

113. TARB was constituted vide UIDAI headquarters office memorandum 18 of 2012. TARB is constituted by UIDAI to manage various aspects of Technology Layer. The Technology layer conforms to the technology aspects of the UID programme and is mainly focused on installation, commissioning and management of CIDR.

114. In 2016 a Committee of officers/representatives of UIDAI was constituted to assess the existing hardware technology with the objectives of (i) Finalization of condemnation policy for IT equipment (ii) Detail of items to be replaced/condemned out of Pre-MSP Contracts along with Quantity (iii) Item wise detail of equipment to be procured with detailed specification of hardware/software with timeline and (iv) cost Benefit analysis for the replacement/ condemned equipment.

ROLE of TARB :

- i. **SLA Supervision**
- ii. **Compliance to Audit recommendations**
- iii. **Optimisation and TCO Management**
- iv. **Technology refresh**
- v. **Providing Micro Inputs for demand forecasting**
- vi. **Approval of capacity planning and cell deployment**
- vii. **Application enhancement and development**
- viii. **Management of Sub- Contractors**
- ix. **Usage of Open Source or free softwares**

Committee Members of TARB:

(a)	Dr Ajay Bhushan Pandey, CEO, UIDAI	---- Chairman
(b)	Dr. Gulshan Rai, NCSC Coordinator	---- Member
(c)	Dr. Rajat Moona, Director IIT Bhilai	---- Member
(d)	Dr. H Krishnamurthy, Professor, IISc	---- Member
(e)	Dr. Manindra Agarwal, Professor, IIT Kanpur	---- Member
(f)	DG NIC	---- Member
(g)	DG CERT-IN	---- Member

(h) Dr. YLP Rao, DDG (Technology), UIDAI --- Convener

115. The committee meets once in a quarter. Additional meetings are convened as per the requirement. The members of the committee outside UIDAI ecosystem sign an agreement with UIDAI to maintain the confidentiality as per the requirement of Aadhaar Act 2016 and Aadhaar Regulations. All required logistics support for the functioning of the committee is provided by UIDAI.

116. Following two external agencies are primarily responsible for conducting assessments and audits of UIDAI infrastructure and ecosystem:

i. **Standardisation Testing and Quality Certification (STQC)**

Standardisation Testing and Quality Certification (STQC) Directorate is an attached office of the Ministry of Electronics and Information Technology, Government of India, provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centres. The services include Testing, Calibration, IT & e-Governance, Training and Certification to public and private organizations. UIDAI has been declared ISO 27001:2013 certified by STQC with respect to Information Security which has added another layer of information security assurance. Further in pursuance of sub-section (1) of Section 70 of the IT Act 2000, UIDAI data has also been declared as **Protected System by National Critical Information Infrastructure Protection Centre.**

STQC is involved with UIDAI in various capacities. Some of the activities are mentioned below:

- a. UIDAI has been **ISO 27001:2013 certified by STQC**. The scope for assessment included the following location – UIDAI Data Centres, SOC and NOC locations and Software Development Centres.

Qualification of auditors: Lead Auditors for ISMS and certified in ISO 27001:2013.

- b. STQC **certifies the biometric devices** to be used for UIDAI enrolment and authentication.
- c. STQC has also conducted **audit of the user acceptance test for IT infrastructure** procurement at UIDAI data centres.

Qualification of Auditors: Lead Auditor, Test Engineer, etc.

ii. **Governance Risk Compliance and Performance Service Provider (GRCP-SP)**

- a. M/s PricewaterhouseCoopers Pvt. Ltd. (PwC) India has been appointed as Governance, Risk, Compliance and Performance Service Provider (GRCP-SP) since October 2015. PwC is acting as an independent monitoring agency to continuously monitor the security of UIDAI ecosystem including CIDR infrastructure, its applications, policies, processes and to monitor UIDAI ecosystem partners for compliance with the Aadhaar Act and its Regulations as well as the defined policies, procedures, guidelines among others.

- b. **Objective:** Objective of GRCP-SP is to provide UIDAI management with oversight of security in UIDAI and security within the ecosystem partners and is expected to measure, monitor and validate that the entire ecosystem is working in a secure manner and as per the laid down regulations, policies, specifications, industry best practices etc.
- c. **Some of the important assessments and activities performed by GRCP-SP include:**
- a) Periodic testing of all UIDAI applications using automated industry standard tools and manual testing by highly skilled technical resources
 - b) Secure code review of all UIDAI applications
 - c) Vulnerability assessment and penetration testing of entire UIDAI infrastructure on a periodic basis
 - d) Network security assessments
 - e) Review of the various security technologies deployed in UIDAI and provide improvement areas
 - f) Review of various encryption applied in UIDAI ecosystem and its effectiveness
 - g) Review of Database and server security
 - h) Biometric security and de duplication assessments
 - i) Conduct a Security gap assessment analysis of the UIDAI Information Security ecosystem.
 - j) Information Security Policy review for the entire set of ecosystem partners of the UIDAI

- k) Undertake risk assessment, assess the existing controls and perform controls gap assessment
- l) SLA measurement framework reviews and SLA process assurance through periodic assessments for all ecosystem partners
- m) Conduct audits for external ecosystem partners including but not limited to Authentication User agencies (AUA), eKYC User Agencies (KUA), Enrolment agencies (EA), among others. Objective of this assessment is to enforce compliance for the ecosystem partners such as AUAs, KUAs and ASAs which use the Aadhaar Authentication services.
- n) Fraud risk assessment and management support

d. Further, for carrying out the above mentioned activities, GRCP-SP has deployed staff with the skillset and adequate expertise.

The key roles defined are as follows:

S.No.	Profile	Area of Expertise and qualification
1	Risk Analyst	Ability to analyze technical and business risks related to security and privacy by taking into consideration multiple, global and local, trends and inputs B.E. / B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent. Preferable: CIRM / CRISC / CITR / CISSP / CISM / CBCP / GIAC / CIRCP / CIPP/IT certification or equivalent
2	Fraud Risk	Should be a seasoned fraud analyst / examiner and

	Analyst	should have experience in handling frauds across multiple industry domains. Should be able to identify and look at a vast array of unstructured data to identify possible fraud and fraud patterns. B.E/B. Tech/B.S / MCA / M.Tech / MBA degree or equivalent. Preferable: CFS/CEH/ GIAC/ GWAPT/ GWEB/ GXPN/ GPEN certification or equivalent.
3	Periodic Compliance Manager	Ability to draw up compliance schedules, compliance checklists to be followed, carrying out compliance and penetration tests, ensuring follow up for closure of identified gaps in terms of deficiencies and deviations, ensuring a regular maturity trend, keeping the team motivated B.E/B. Tech/B.S / MCA/ M. Tech / MBA degree or equivalent. Should be a certified auditor. Preferable: BS7799 Lead Auditor/ CISA/ CISM/ CISSP / CBCP / DRCS / CISRCP / CAST / GIAC/ CSCS / CBP / CBSE/ GPEN / GWAPT / GWEB / CASS / CIPP/IT certification or equivalent. ology, well versed with various tools used for protection of networks and related components from a security perspective
4	Network Security Auditor	Deep understanding of network security, protection of networks using controls related to people process and technology. B.E/B. Tech / B.S / MCA / MBA/ M. Tech degree or equivalent. Should be a certified auditor. Preferable: CISSP / BS7799 Lead Auditor/ CISM/CEH / GPEN/ GCFW/ CCNA/ CCNP/ CCSE / CCSA certification or equivalent

5	Application Security Auditor	Excellent understanding of application security and privacy impact assessment in each phase of the software development lifecycle, excellent understanding in Java security B.E/B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent Should be a certified auditor. Preferable: GWEB / CASS / GWAPT/ BS7799 Lead Auditor/ CISM / CISSP / CCSK / CIPP/IT certification or equivalent.
6	Database Security Auditor	Well versed with aspects of database security and privacy, access control, identity management, biometric storage, encryption of database, data obfuscation techniques. Has deep security related knowledge of Oracle, My SQL and SQL databases. B.E/B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent Should be a certified auditor. Preferable: BS7799 Lead Auditor/ CISSP / CISM / CISA/ CDRP/ CIRM / CBP / CBSE / CIPP/IT certification or equivalent.
7	Manager Partner Ecosystem Field Audit	Security Audits B.E. / B. Tech / B.S / MCA degree or equivalent. Preferable: CISA / CISSP / ITIL certification or equivalent
8	Partner Ecosystem Field Audit	Security Audits B.E. / B. Tech / B.S / MCA degree or equivalent. Preferable: CISA / CISSP / ITIL certification or equivalent
9	SOC Manager	Security products and technologies; security engineering, networking protocols and data center;

		security analysis and investigations B.E. / B. Tech / B.S / MCA / M.Tech / MBA degree or equivalent. Should be an experienced IT Security practitioner. CISSP, CISM or equivalent certification
10	IAM Manager	Requirements gathering and definition, review of security design and specification, development, testing, and implementation support B.E. / B. Tech / B.S / MCA / M.Tech / MBA degree or equivalent. Should be an experienced IT Security practitioner. CISSP, CISA or equivalent certification preferred

Security of the authentication eco-system:

- a. **Secure Channel:** Access to UIDAI's Central Identity Repository is available only to authorized Authentication User Agencies (AUAs) and e-KYC User agencies (KUAs) through authorized Authentication Service agencies (ASAs) which have establish secured wired network connectivity for the purpose of authentication with the Central Identities Data Repository (CIDR), in compliance with the Regulations, specifications, standards and technology architecture as prescribed by UIDAI, from time to time. Further, CIDR is accessible only through APIs defined by UIDAI and authentication request have to be in the format as prescribed by UIDAI.
- b. **Identity data is always encrypted:** UIDAI mandates that the authentication application shall immediately package and encrypt the

input parameters including biometrics into personal identity(PID) block before any transmission, as per the specifications laid down by UIDAI. Therefore, resident's identity data traverse from authentication device to CIDR only in encrypted form. The Authentication request and response are always digitally signed to establish its authenticity and integrity.

- c. **Encrypted eKYC response:** The eKYC response is from UIDAI CIDR is always encrypted and only the KUAs ie requesting entities can decrypt it with their private keys.
- d. **Audit data:** The audit data containing request and response is stored for 6 months online and 5 years offline for any grievance resolution. The PID data is always kept in encrypted form in Audit.
- e. **Use of Hardware security module (HSM) :** All the keys are stored in secure appliance called HSM in CIDR and no key can be taken out from this appliance.
- f. **Use of License key by AUA/KUA/ASA:** The authorized requesting entities are allowed to generate their own license key on UIDAI's portal which is part of every Auth request and is validated in CIDR before responding to Auth requests.
- g. **STQC certified biometric devices:** UIDAI has mandated use of only Standardisation Testing and Quality Certification (STQC) certified biometric devices for all authentication requests.
- h. **Multi-factor authentication:** UIDAI provides multiple ways of authentication such as demographic, biometric (Fingerprint/Iris), OTP or a combination of these factors. Further, the Authentication User Agency may decide to use additional authentication factors on

their own depending on their security need and business requirements.

- i. **Biometric locking:** Some residents might be having the apprehension that any unscrupulous element may capture their biometrics (Fingerprint / Iris) and use it for fraudulent Aadhaar Authentication. UIDAI has provided the facility to protect against an eventuality whereby residents can lock their biometrics and whenever they need to do Aadhaar authentication using biometrics, it can be unlocked for a specified short period of time.
- j. **Alert notifications:** UIDAI provides instant e-mail alert notifications to Aadhaar number holder for biometric authentication with details such as time of authentication, mode of authentication, the name of Authentication user agency through which authentication has happened, UIDAI's response (Yes or no) and contact details of UIDAI. Therefore, in case of any issues with the transaction, Aadhaar number holder may approach UIDAI or the Authentication user agency.
- k. **Fraud detection and prevention:** UIDAI keeps on doing analysis on the transactions performed by various AUAs and based on the requirement keeps on adding new features or rules to ensure increased security of authentication transactions. AUAs are also advised to perform analysis on the transactions to monitor and avoid any irregular or fraudulent activity
- l. The CIDR has been designed so that it is bifurcated into two distinct systems - the Authentication system and the Enrolment system. Only encrypted data from registered operators of enrolling

agencies are allowed to enter the Enrolment System, after passing a rigorous check at the firewall surrounding this system. This firewall acts like a one-way software valve and ensures that data can only enter but cannot leave.

m. The resident data packets are transported in encrypted form until it passes through the firewall within the physical premises of the CIDR. This encrypted data can only be decrypted by the Hardware Security Module (HSM) that is physically located inside the CIDR. The HSM is completely isolated from the public internet. It is designed to self-destruct if any attempts are made to attack it.

n. The Authentication system allows for two-way traffic to and from the CIDR. However, authentication can only be carried out on requests initiated by AUAs or KUAs who in turn cannot directly access the database but have to do so through the infrastructure provided by ASAs. These ASAs maintain dedicated infrastructure solely for the purpose of connecting the AUAs to the Aadhaar database. Thus, access to the Authentication CIDR is not available over the public internet. The UIDAI has created a private network for the purpose of accessing the Authentication CIDR. Access to this Aadhaar internet is limited to only registered entities and all authentication transactions that take place on it are logged and capable of being attributed. As a result, this system is secure from attacks through the public internet.

o. All devices that collect biometric or demographic information must be registered with the UIDAI and the CIDR will refuse to accept authentication requests made by requesting entities using

unregistered devices. All communication to and from the CIDR database is encrypted with a high level of encryption making it impossible for any third party to read any of this information. The entire CIDR system is maintained in a highly secure physical environment with high security and very limited access to authorised personnel being allowed into the premises.

117. Under paragraph 16(vii), the Petitioner has enumerated the main headings under which the pleadings in the writ petition are arranged. The said paragraph is being reproduced here for this Hon'ble Court's reference-

"vii. In order to make for an easier perusal of this petition, the pleadings are arranged under the following main headings:

- (A) Security Breaches and Statutory Provisions Violated;*
- (B) Data Protection Duties under the law;*
- (C) Appointment of Investigative/Audit Committee;*
- (D) Constitutional/Common Law Rights and Damages;*
- (E) The Right to Know; and*
- (F) The Right to Legal Redressal."*

In addition to the submissions so far made in the present Reply in this regard, Respondent humbly submits as follows-

(A) Security Breaches and Statutory Provisions Violated'-

118. That all the allegations in the writ petition under the heading '(A)- Security Breaches and Statutory Provisions Violated' are vehemently

denied as false and misleading. It is submitted that UIDAI vide their press release dated 04 Jan 18 has categorically denied any data breach of Aadhaar Data by giving the following clarifications on the subject:-

- i. Unique Identification Authority of India (UIDAI) has denied the media report published in The Tribune titled "Rs 500, 10 minutes, and you have access to billion Aadhaar details" and has said that it is a case of misreporting. UIDAI assured that there has not been any Aadhaar data breach. The Aadhaar data including biometric information is fully safe and secure. In a statement issued UIDAI said that UIDAI has given the said search facility for the purpose of grievance redressal to the designated personnel and state government officials to help residents only by entering their Aadhaar number/EID. UIDAI maintains close scrutiny over any misuse which can be traced and appropriate action taken.
- ii. UIDAI further clarified that the reported case appears to be instance of misuse of the grievance redressal search facility. As UIDAI maintains complete log and traceability of the facility, the legal action including lodging of FIR against the persons involved in the instant case has been done. UIDAI reiterates that the grievance redressal search facility gives only limited access to name and other details and has no access to biometric details. UIDAI reassures that there has not been any data breach of biometric database which remains fully safe and secure with highest encryption at UIDAI and mere display of demographic information cannot be misused without biometrics.

- iii. UIDAI also mentioned that, the Aadhaar number is not a secret number. It is to be shared with authorized agencies whenever an Aadhaar holder wishes to avail certain service or benefit of government welfare scheme/s or other services. But that does not mean that the proper use of Aadhaar number poses a security or financial threat. Also, mere availability of Aadhaar number will not be a security threat or will not lead to financial/other fraud, as for a successful authentication, fingerprint or iris of individual is also required.
119. Therefore, the claims of bypassing or duping the Aadhaar enrolment system are totally unfounded. Aadhaar data is fully safe and secure and has robust uncompromised security. The UIDAI Data Centres are infrastructure of critical importance and are protected accordingly with technology conforming to the best standards of security and also by legal provisions.
120. It is further humbly submitted that the facility provided by UIDAI was only for search and no one could make any changes in the database maintained by UIDAI. Logs were enabled for the portal and hence, any transaction done by any of the user could be traced for specific action. Moreover, an FIR has been filed and the matter is under investigation.
121. The contentions regarding violation of statutory rules are also specifically and strongly denied. It is reiterated that there has been no leakage from the CIDR database. The Aadhaar ecosystem is robust and no breaches of Aadhaar data have taken place. The contention of the Petitioner that a number of statutory duties under both Aadhaar Act and IT Act as well as their cognate rules and regulations have been violated

is baseless, perfunctory and devoid of merit. Petitioner is merely reiterating the obligations of Respondents as laid down in the Aadhaar Act, which the Respondents have always complied with.

122. As far as the security procedures applicable to third party affiliates is concerned, it is submitted that the Ecosystem partners are bound by Aadhaar Act and Regulations. UIDAI has taken very robust measures to ensure compliance by all the third party partners/ affiliates etc. These are reflected in the various regulatory, policy, governance and enforcement measures taken by UIDAI from time to time.

123. As per Regulation number 6 of Aadhaar (Data Security) Regulations, 2016, the ecosystem partners have to get themselves audited and UIDAI also conducts audit as and when required. The ecosystem partners are audited by UIDAI in compliance of the Aadhaar Act and Regulations as well as its Information security policy and procedure at regular intervals. UIDAI has defined an Information Security Policy for its internal as well as external ecosystem partners. The internal policy is applicable to the CIDR and the personnel of UIDAI while external policy is applicable to the external ecosystem partners. The policy includes controls to ensure security and confidentiality of resident data. UIDAI has also defined non-disclosure and confidentiality clauses in the agreements signed with various third parties/ affiliates to enhance security. Any non-compliance is viewed seriously and defaulters are required to take corrective action / penalised as required as per the provisions of the Aadhaar Act, 2016 and its Regulations framed there under.

The clause under which the assessments are mandated are:

“(1) All agencies, consultants, advisors and other service providers engaged by the Authority, and ecosystem partners such as registrars, requesting entities, Authentication User Agencies and Authentication Service Agencies shall get their operations audited by an information systems auditor certified by a recognised body under the Information Technology Act, 2000 and furnish certified audit reports to the Authority, upon request or at time periods specified by the Authority.

(2) In addition to the audits referred to in sub-regulation (1), the Authority may conduct audits of the operations and systems of such entities or persons, either by itself or through an auditor appointed by the Authority.”

124. Hence, all the agencies have to get themselves audited through an Information Systems auditor and furnish the audit report. UIDAI has also performed security audits of a number of ecosystem partners on sample basis either through itself or auditor appointed by UIDAI. These ecosystem partners include but are not limited to enrolment agencies and enrolment centers, Authentication User Agencies (AUAs)/ Sub-Authentication User Agencies (Sub-AUAs) / Authentication Service Agencies, Logistic Service Provider, Contact Centre, etc.

125. Any non-compliance or issues observed in the processes and functioning of the agency are highlighted to ensure the agency complies with the requirements. Appropriate corrective actions/ fines/ penalties are also imposed on such agencies as required.

126. Moreover, UIDAI has defined an Information Security Policy for its internal as well as external ecosystem partners. The internal policy is applicable to the CIDR and the personnel of UIDAI. While the external policies have been defined for the various third party partners and affiliates. However, the policy cannot be shared in the public domain as per Regulation 7 of the Aadhaar (Data Security) Regulations, 2016 which states as follows:

“All procedures, orders, processes, standards and protocols related to security, which are designated as confidential by the Authority, shall be treated as confidential by all its personnel and shall be disclosed to the concerned parties only to the extent required for giving effect to the security measures. The nature of information that cannot be shared outside the Authority unless mandated under the Act includes, but not limited to, Information in CIDR, Technology details, Network Architecture, Information security policy and processes, software codes, internal reports, audit and assessment reports, applications details, asset details, contractual agreements, present and future planned infrastructure details, protection services, and capabilities of the system.”

127. Nevertheless there are various other measures mentioned on UIDAI main website which provide an idea on the high level measures taken by UIDAI including ISO27001:2013 certification to ensure security and privacy of data.

100

128. Apart from this, UIDAI releases various circulars on security and privacy enforcement in the ecosystem. These circulars are available in the public domain and are mentioned as follows:

- a. Aadhaar Authentication API specification version 2.5, Aadhaar eKYC API specification version 2.5 and Aadhaar OTP request API specification version 2.5 include requirements on encryption of data at the time of capture, use of https protocol, AES 256 for symmetric encryption and RSA 2048 for public key encryption, prohibition on storage of PID block on any device or server etc.
- b. Aadhaar Registered devices Technical specifications – version 2.0 and Circular for Registered devices dated 25.01.2017: UIDAI mandated all AUAs, KUAs and STQC certified device providers to get their devices certified as Registered devices by 31-May-2017. Registered devices enforced device identification and eliminated the possibility of stored biometrics by AUAs and KUAs
- c. Implementation of HSM AUA/KUA/ASA dated 22.06.2017: UIDAI mandated that all AUAs/KUAs/ASAs shall use Hardware based Security Module (HSM) for digital signing of Auth XML and decryption of e-KYC data.
- d. Circular for Reference key dated 25.07.2017 and Frequently asked questions for Aadhaar vault and Reference keys dated December 2017: In order to enhance the level of security for storing Aadhaar numbers, all agencies collecting, storing, processing Aadhaar numbers were mandated to implement reference keys mapped to Aadhaar numbers through tokenization in all systems.

e. Dos and Dots for Aadhaar User agencies/Departments dated October 2017: UIDAI issued guidelines on enhancing the security of Aadhaar numbers through masking, encryption, and implementation of HSM for encryption key management

129. As far as the position of the answering Respondent/UIDAI as a Custodian under Regulation 3 of Aadhaar Data Security Regulations 2016 is concerned, it is humbly submitted that a 'custodian' means a person entrusted with the custody or care of something. Thus in reference to Annexure P-7, UIDAI has specified that "the data pertaining to residents is held by UIDAI as a trustee /custodian, and is not shared with any agency without the consent of the resident, either in writing or when electronically authenticated. The Aadhaar is activated only at the request of the Aadhaar holder. He/ She may choose to let it be dormant by not using it at all. As a trusted custodian, the residents' data has always been handled in a responsible manner with state-of-the-art security systems in place in the UIDAI." Thus the contents of the referred FAQ should be read in line with the provisions of Aadhaar Act and submissions made herein.

130. Petitioner's contention regarding lack of a security policy is also strongly denied and, it is submitted that UIDAI has defined an Information Security Policy for its internal as well as external ecosystem partners. The internal policy is applicable to the CIDR and the personnel of UIDAI, while the external policies have been defined for the various third party partners and affiliates. However, as stated in the preceding paragraphs above, the policy cannot be shared the public

102

domain as per Regulation 7 of the Aadhaar (Data Security) Regulations, 2016.

131. Further Section 30 of the Aadhaar Act Section 30 states as follows-

“.....The biometric information collected and stored in electronic form, in accordance with this Act and regulations made thereunder, shall be deemed to be “electronic record” and “sensitive personal data or information”, and the provisions contained in the Information Technology Act, 2000 and the rules made thereunder shall apply to such information, in addition to, and to the extent not in derogation of the provisions of this Act.”

132. It is also relevant to mention here that UIDAI CIDR is ISO27001:2013 certified since 2015 and goes through yearly surveillance audits from STQC. All the processes of UIDAI have been developed keeping in mind the ISO 27001 standards.

133. That the Petitioner is seeking damages under Section 43A of the IT Act and compensation alleging wrongful loss to Aadhaar number holders due to security breaches. However, Petitioner has not given details of any actual legal injury caused to him and therefore a claim for damages is totally baseless and unsustainable.

134. The answering Respondent further vehemently denies the contention of the Petitioner that the architecture of Aadhaar permits the mere entry of an Aadhaar number as a password to access confidential demographic data. In fact, under the Aadhaar Act, even Biometrics are not being used as a password and are merely used for authentication/identification of a person and not for authorization of transactions.

135. It is also respectfully submitted that UIDAI has adequate controls to prevent against such possibilities. These controls include registered devices, biometric locking, multi-factor authentication, resident notification and Aadhaar number locking. In addition, Authentication in UIDAI is through an assisted model which dissuades a fraudulent activity. Use of false iris copies for authentication would require collusion of AUA operator and any such act is punishable under Aadhaar Act, 2016. That apart from the capability of preventing such possibilities, UIDAI has built systems based on fraud analytics to be able to detect any such occurrence of suspicious activities. UIDAI offers a much more secure method of authentication than the traditional systems and technologies prevalent before Aadhaar which have proven to be filled with multiple possibilities of fraud already and UIDAI, through technology, is offering the most secure means of identity verification, which even the Hon'ble Supreme Court has acknowledged and taken judicial notice of.
136. That the allegation that the Respondent No.1 and its affiliates have violated important security standards outlined in the RSP Rules is also vehemently denied, and it is submitted the petitioner has taken a limited view of the various privacy and security measures taken by UIDAI and has failed to understand these measures. UIDAI has taken all necessary measures that are required to ensure the security and privacy of resident information. Further, UIDAI constantly ensures compliance with the changing technological and legal landscape and ensures Aadhaar Act fulfils the relevant requirements.

137. UIDAI has also published various privacy and security measures for the residents to access on its main website. Following are some examples of information available in an easy and accessible manner to the residents as per the requirement of the section 43A of the IT Act 2000. Example:

<https://uidai.gov.in/your-aadhaar/faqs.html>

138. Also, as stated earlier, UIDAI CIDR is ISO27001:2013 certified since 2015 and goes through yearly surveillance audits from STQC. All the processes of UIDAI have been developed keeping in mind the ISO 27001:2013 standard. ISO27001 is also mentioned as a standard to showcase reasonable security practices under the IT Rules 2011 (Reasonable security practices and procedures) created under section 43A of the IT Act 2000. Hence, UIDAI is following all reasonable security practices and procedures for compliance to section 43A of the IT Act 2000.

139. Petitioner's contention that the Respondent herein has failed to lay down an information policy for itself and its operations, is also vehemently denied. It is submitted that protecting resident data and thereby ensuring confidentiality and privacy is paramount as per the provisions of the Aadhaar Act. Information security has been engraved in the design of Aadhaar. Section 28 of the Aadhaar Act provides that the Authority (UIDAI) shall ensure that the information in the possession or control of the Authority including the information stored in the CIDR is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder and against accidental or intentional destruction, loss or damage. Various

security provisions have been included in the Aadhaar regulations such as Aadhaar (Enrolment and update) regulations, Aadhaar (Authentication) regulations, Aadhaar (Data security) regulations and Aadhaar (Sharing of information) regulations.

140. It is further respectfully submitted in reply to the contention that the answering Respondent has failed to publish its privacy policy on its website as per Rule 4 of the RSP Rules, that the Petitioner has taken a limited view of the various privacy measures taken by UIDAI and these are easily available in the public domain.

141. UIDAI has defined an Information Security Policy based on ISO standards. All the requirements of ISO 27001 standard are complied with and are updated on a periodic basis as per the need. Thus, the following processes have been kept in place for achieving such compliance-

- a. UIDAI has prepared the Information Security Policy for its internal as well as external ecosystem.
- b. UIDAI CIDR is ISO27001:2013 certified since 2015 and goes through yearly surveillance audits from STQC.
- c. Information Security risk assessment is conducted on a periodic basis to identify the risks facing UIDAI and take appropriate measures to address these.
- d. Multiple security committees exist to take decisions on aspects related to the technology and security of Aadhaar with well-defined roles and responsibilities.
- e. UIDAI has a well-established audit program where audits are conducted by both internal as well as external agencies. The audits

are held for the various security products, network, applications, etc. and issues identified are addressed promptly.

142. The contention that the Respondent therein has failed to implement information security risk assessment process is also strongly denied. Information security risk assessment exercises are conducted periodically and the same are acted upon by respective stakeholders. Such risk assessment is conducted as per industry best practices and ISO standards.
143. With respect to the contention that it is not clear whether audits were carried out regularly by the Respondent herein, it is humbly submitted that periodic security audits are conducted by UIDAI for both its internal as well as external ecosystem. These audits are conducted either by UIDAI itself or third party auditor appointed by UIDAI. Subsequently, all the third party partners/ affiliates are also required to perform the security audit of their operations and functions as per Regulation number 6 of Aadhaar (Data Security) Regulations, 2016.
144. Petitioner has also sought appointment of a committee to ascertain robustness of the security systems and processes instituted by the Respondent herein. In this regard, it is submitted that UIDAI already has number of committees for the purpose of security in UIDAI with various mandates. These committees are responsible to ensure high standards of review, governance and advice on cybersecurity, technology and privacy matters of Aadhaar.
145. Petitioner has further alleged that the Respondent herein has failed to put in place basic tenets of a reasonable security policy. The said contention is vehemently denied and it is submitted that all the

necessary security control and reasonable security practices have been put in place by UIDAI. As informed by UIDAI vide its press release:

“UIDAI has given the said search facility for the purpose of grievance redressal to the designated personnel and state government officials to help residents only by entering their Aadhaar number/EID. UIDAI maintains complete log and traceability of the facility and any misuse can be traced and appropriate action taken. The reported case appears to be instance of misuse of the grievance redressal search facility.”

146. The Petitioner has sought to contend that he should be compensated for the wrongful loss caused to him by the alleged security breaches. However there is no mention whatsoever of any personal wrongful loss suffered by the Petitioner and such a grievance is only a figment of Petitioner's imagination.
147. Further, the contention that there are no specific remedies under the Aadhaar Act for breach of privacy, are completely false and baseless. It is submitted that the Aadhaar Act lays down penalties for unauthorized sharing of residents' identity information, failure to keep eKYC data secure, failure to properly inform the residents about the use of their information, or failure to obtain their consent for authentication. The non-compliant individuals or entities may receive monetary penalty (up to one lakh rupees) and/or imprisonment (up to 3 years) which may vary depending upon the severity and impact of the violation. Some of the relevant sections include:
- a. Section 34: Penalty for impersonation at time of enrolment)

108

- b. Section 35: Penalty for impersonation of Aadhaar number holder by changing demographic information or biometric information
 - c. Section 36: Penalty for impersonation
 - d. Section 37: Penalty for disclosing identity information
 - e. Section 38: Penalty for unauthorized access to the Central Identities Data Repository
 - f. Section 39: Penalty for tampering with data in Central Identities Data Repository
 - g. Section 40: Penalty for unauthorized use by requesting entity
 - h. Section 41: Penalty for non-compliance with intimation requirements
 - i. Section 42: General Penalty
 - j. Section 43: Offences by Companies
 - k. Section 44: Act to apply for offence or contravention committed outside India
148. That in reply to the contentions under the sub-heading “A2. Srivastava Spoof”, the answering Respondent vehemently refutes that Mr. Abhinav Srivastava carried out e-KYC transactions using the CIDR database. The Aadhaar ecosystem is robust and no breaches of Aadhaar data have taken place.
149. It is submitted that a mobile application namely “Aadhaar e-KYC Verification” available on Google Play Store was using an NIC platform for providing authentication and e-KYC API services in an unauthorized manner. Mr. Abhinav Srivastava of “Qarth Technologies Private Limited” developed a mobile application, namely, “Aadhaar e-KYC Verification”, which was made available on Google Play

store,(https://play.google.com/store/apps/details?id=mygov.aadhaar.ekyc&hl=en).

150. It is reiterated that UIDAI server has not been breached. Initially, an FIR was filed by UIDAI as this activity of the above web service provider involved the violation of the Aadhaar Act, 2016 and a criminal case, vide, FIR no.0130/ 2017 dated 26.07.2017 was registered at the Seshadripuram Police Station in Bengaluru City.
151. Even though Respondent No.3/NIC is a KUA and authorised to carry out e-KYC authentication, however, e-KYC authentication cannot be done directly as there is an intermediary ASA between the UIDAI server and KUA. Further, no user agencies, whether KUA or ASA, are allowed access into the UIDAI databases and the services for AUA are limited only to the extent of getting a “yes” or “no” response after authentication. It is reiterated that no entity can gain access of CIDR database and the same is fool-proof.
152. Regarding the modus operandi of Mr. Abhinav Srivastava, it is respectfully submitted that he had misused the NIC platform and such misuse of the NIC platform and authentication services was unauthorised and punishable in law.
153. The NIC platform was misused by Mr. Abhinav Srivastava and as soon as it came to the notice of NIC, the web services/API were stopped immediately. There has been no breach of the UIDAI server. As Mr. Abhinav Srivastava was unauthorisedly providing Aadhaar e-KYC verification on Google Play Store, as stated earlier, UIDAI filed a complaint and an F.I.R no. 130/2017 dated 26.07.2017.

154. Therefore, any media report suggesting or indicating a breach of the UIDAI's Aadhaar database or CIDR is incorrect as not a single case of identity theft or financial loss due to Aadhaar has been reported. It cannot be stressed upon enough that Aadhaar data is fully safe and secure and UIDAI data centre has had robust uncompromised security all throughout.
155. In response to the contentions under the sub-heading "A.2.1.-provisions violated", it is submitted that in the Abhinav Srivastava incident, the application of NIC, i.e. Online Registration system (ORS) was providing services to the end user based on OTP authentication (OTP is received on the Registered mobile) which implies that the user availing the service has to do an affirmative action of providing his / her Aadhaar number and then provide the OTP to the ORS application to avail the service.
156. The developer Abhinav Srivastava, utilized this application to extend authentication services to users by providing a separate front end wrapper. However still the users had to consciously provide the Aadhaar number and OTP to this extended application to avail the service provided by this extended application hence this action could not have been done without user's explicit knowledge and consent. Hence, Abhinav Srivastava could not have performed e-KYC authentication without participation of the Aadhaar number holder through this extended application as it requires submission of Aadhaar number and OTP received on registered mobile to access the identity information. Further, UIDAI provides a high level security for all

authentication requests. There are multiple layers of security for each authentication requests

157. That as far as the allegation of the Petitioner that the answering Respondent herein failed to secure the API and its token/key is concerned, apart from the submissions made under paragraph 71 of this Affidavit, it is humbly submitted that in addition to the app, the developer had an unauthorized access to NIC server (an authorized AUA of UIDAI) and was providing illegal Aadhaar verification services. This was in complete violation of Section 40 of The Aadhaar Act, 2016 and Aadhaar Regulation framed there under and therefore an FIR was promptly filed against him by the UIDAI.
158. Further, various security guidelines and mandates are issued to agencies handling the Aadhaar related data from time to time to ensure they comply with the provisions of the Aadhaar Act and Regulations. The Aadhaar ecosystem partners are also audited at regular intervals to ensure compliance and any non-compliance is viewed seriously and defaulters are required to take corrective action / penalised as per the provisions of the Aadhaar Act, 2016 and its Regulations framed there under.
159. It is respectfully submitted that the Abhinav Srivastava incident is a mischievous and illegal access of NIC's infrastructure rather than sharing of license keys. Further the impact of the illegal provisioning of Authentication service through NIC in this incident has been exaggerated by the Petitioner.
160. In reply to the contentions under the sub heading "A.2.1.3-Failure to systematically audit and track breaches", it is submitted that UIDAI has

taken all necessary governance measures to ensure security within the ecosystem as already stated above. UIDAI has defined several provisions for the audit of the AUA/KUA and other agencies.

161. Regulation 19(g), Aadhaar (Authentication) Regulations, 2016 – *An Authentication Service Agency shall ensure that its operations are audited by an information systems auditor certified by a recognized body on an annual basis, and provide a certified audit report, to the Authority, confirming its compliance with the policies, processes, procedures, standards, or specifications, issued by the Authority in this regard, from time to time;*

162. Regulation 21, Aadhaar (Authentication) Regulations, 2016 - *Audit of requesting entities and Authentication Service Agencies-*

“(1) The Authority may undertake audit of the operations, infrastructure, systems and procedures, of requesting entities, including the agencies or entities with whom they have shared a license key or the entities on whose behalf they have performed authentication, and Authentication Service Agencies, either by itself or through audit agencies appointed by it, to ensure that such entities are acting in compliance with the Act, rules, regulations, policies, procedures, guidelines issued by the Authority.

(2) The Authority may conduct audits of the operations and systems of the entities referred to in sub-regulation (1), either by itself or through an auditor appointed by the Authority. The frequency, time and manner of such audits shall be as may be notified by the Authority from time to time.

(3) An entity subject to audit shall provide full co-operation to the Authority or any agency approved and/or appointed by the Authority in the audit process, and provide to the Authority or any agency approved and/or appointed by the Authority, complete access to its procedures, records and information pertaining to services availed from the Authority. The cost of audits shall be borne by the concerned entity.

(4) On identification of any deficiency by the Authority, the Authority may require the concerned entity to furnish necessary clarifications and/or information as to its activities and may also require such entity either to rectify the deficiencies or take action as specified in these regulations.”

163. In the FIR filed by NIC it has been stated that the Aadhaar e-KYC Verification app was not uploaded by NIC on the Google Play Store and hence was not authorized to access NIC's authentication services. Hence, this access by developer amounts to unauthorized and illegal access to NIC. Additionally NIC had completed an Audit of the said application as per the process on 25 January 2017 and UIDAI had conducted an audit of NIC as AUA/KUA in May 2016 as part of the periodic sample audits.

164. In response to the allegations under the sub-heading “A.2.1.4-Failure to deploy a fraud analytics system”, the said allegation is denied as incorrect and it is humbly submitted that UIDAI has taken all necessary governance measures for the ecosystem to ensure that frauds are detected and prevented and that there is a continuous improvement process. UIDAI requires the ecosystem partners to setup strong anti-

fraud mechanisms under the Aadhaar regulations. Following are the regulations that aim at preventing and redressing incidents of fraud -

- a. Regulation number 3 (2) (g), Aadhaar (Data Security) Regulations, 2016 – “measures for fraud prevention and effective remedies in case of fraud;”
- b. Regulation number 14 (1) (l), Aadhaar (Authentication) Regulations, 2016 – A requesting entity shall inform the Authority of any misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within their network. If the requesting entity is a victim of fraud or identifies a fraud pattern through its fraud analytics system related to Aadhaar authentication, it shall share all necessary details of the fraud with the Authority.

165. In reply to the allegations in the petition under the sub headings “A.2.2- Other Violations” and “A.2.3-action against NIC”, the contents of earlier paragraphs of this Affidavit may be referred to, as the same are not being repeated for the sake of brevity.

166. The answering Respondent further vehemently denies the contentions of the Petitioner under the sub-heading “A.3 -Breach: Publication of Aadhaar data”.The answering Respondent further submits in this regard that it was found that approximately 210 websites of Central Government, State Government departments including educational institutes, were displaying the list of beneficiaries along with their name, address, other details and Aadhaar numbers for information of general public.Aadhaar and other personal data was removed from the said websites. In this regard, Ministry of Electronics and IT (MeitY)

has issued OM no. 10(36)/2015-EG-II (Vol-V) dated 25 March 2017 regarding "Data Sharing – Compliance of the IT Act, 2000 and Aadhaar Act, 2016" and subsequently D.O. No. NIC/DDG (SBS)/ITACT/2017 dated 24 April 2017 regarding "Sensitization on compliance of IT Act, 2000 and Aadhaar Act, 2016 while Data Sharing in the Departmental Websites".

True Copy of the OM Dated 25.3.2017 and D.O. dated 25.03.2017 are marked as **Annexure R-13**

167. That the allegations contained in sub-heading A.4 (Breach: The Biometrics Frauds), are vehemently denied. As far as the allegations pertaining to e-KYC user agencies namely Axis Bank Limited, Suvidhaa Infoserve Private Limited and eMudhra Limited are concerned, it is submitted that the UIDAI has conducted thorough enquiries and wherever necessary, suitable actions have been taken under the Aadhaar Act, 2016 and the Regulations therein.

168. Thus, as stated above, Notices were issued under Regulation 25 of the Aadhaar (Authentication) Regulations, 2016 to M/s Axis Bank Limited, M/s eMudhra Consumer Services Limited and M/s Suvidhaa Infoserve Pvt. Ltd. UIDAI had also initiated action under Indian Penal Code, Information Technology Act, 2000 and Aadhaar Act, 2016 by filing an FIR dated 24.02.2017 with Kamla Market Police Station in this matter. Subsequently, the license key of M/s Suvidhaa Infoserve Pvt Ltd. was suspended and disincentive of Rs. One Crore was imposed. The AUA Agreement of M/s Suvidhaa Infoserve Pvt Ltd was also terminated. License key of M/s eMudhra Consumer Services

Limited was revoked and disincentive of Rs. One Crore was imposed. After corrective measures were taken by the entity along with making part payments of the disincentive in instalments, their license key was restored. License key of M/s Axis Bank Limited was revoked and disincentive of Rs. One Crore was imposed. After corrective measures taken by the entity along with making full payment of the disincentive, their license key was restored.

169. Further, UIDAI has launched the registered devices to control the security of biometric information captured during authentication. Registered devices specification addresses precisely the scenario when AUA device or host machine is compromised. In registered devices it is ensured that biometrics data between device and host is encrypted and devices are uniquely identified. It provides the following key security features:

- a. Device identification – every physical sensor device having a unique identifier that is pre-registered which can be strongly authenticated. This allows every transaction to be traceable to unique physical device and also allows advanced device level analytics and fraud management.
- b. Eliminating use of stored biometrics – every biometric record (FMR, FIR, IIR) is processed and encrypted within the sensor device eliminating transmission of unencrypted biometrics from sensor to host machine.

170. A standardized Device Driver is provided by the device providers that is certified. This device driver (exposed via an SDK/Service) encapsulates the biometric capture, any user experience while capture

(such as preview), and signing and encryption of biometrics all within it.

Following are additional features of registered devices

- i. Tamper Resistant Security Module (TRSM)
- ii. Unique Physical ID
- iii. Secure Storage for storing encryption keys and device registration ID
- iv. RAM and Storage – RAM to process images and flash to keep public key
- v. TRNG – Capability to generate True Random number as per NIST
- vi. Encryption, Hashing and Signature
- vii. Firmware APIs

171. It is further submitted that UIDAI had discontinued the use of non-Registered Devices and access to Auth API 1.6 for all AUAs w.e.f. 01.05.2018 and currently, all the biometric authentication transactions are performed on Registered Devices only.

172. The contentions under the sub-heading “A.5-Other Breaches and Security Concerns” are vehemently denied. It may be noted that SRDH facility was earlier made available to few state governments. This was meant for repository of demographic data along with photograph of residents of the state for seeding of Aadhaar data in various applications / schemes of the state. However, after the Aadhaar Act, 2016 was notified, UIDAI has stopped extending this facility. This issue was argued by the Petitioners in the Supreme Court in the case of Puttaswamy and Affidavits were filed by the respondents to

demonstrate that any biometric data stored by the States were destroyed and certificates obtained from the concerned States.

173. The Petitioners have alleged that the Biometric Data which was collected at the time of enrolment by the Registrars prior to the enactment of the Aadhaar Act were being retained by the concerned State Governments/Registrars. After the provisions of the Aadhaar Act came into force with effect from 12.09.2016 and especially in light of Section 29(1) of the Aadhaar Act, 2016 it contained a clear prohibition against sharing of Biometrics with anyone for any reasons whatsoever and that it should only be used for the purpose of generation of Aadhaar and authentication under the Act. Therefore, in accordance with the above requirement of law, the UIDAI had issued a circular dated 17.04.2017 pursuant to its powers under Regulation 11 of the Aadhaar (sharing of information) Regulation, 2016 directing that the registrar packets, if any, available with the Registrars or any other agencies or their service providers authorized by the Registrar shall be destroyed by them in presence of a team of Officers from UIDAI not later than 30.04.2017. The Registrar shall also provide a certificate that they have destroyed the Registrar packet and that no Registrar Packet is available with them in the attached template. As per the circular after the destruction, the Registrar shall handover the keys (private keys) of the Registrar Packet to the UIDAI team. In light of the above, it is submitted that most Registrars confirmed that they did not ever retain any biometric data and as for the rest, all State Government Registrars and State instrumentalities who were Registrars have destroyed

biometric data in their servers which were collected during Aadhaar enrolment.

174. Illustratively, the Government of Maharashtra has issued a Certificate dated 23.06.2017 stating that no such Registrar Packets containing personal information of residents including sensitive Biometric information was found in the servers.
175. The IDBI Bank vide its Letter dated 25.04.2017 has also confirmed that as a Registrar, it has not preserved any Resident Data as Registrar Packet including Biometrics and KYR+ of any Resident irrespective of whether it is a bank customer or not.
176. A Certificate dated 28.04.2017 by Dena Bank certifies that Dena Bank is not holding any packets, particularly Biometrics, and other identity information collected as part of the process of Aadhaar Enrollment in its possession.
177. A Letter dated 27.04.2017 by the Jharkhand Agency for Promotion of Information Technology (JAP-IT) established under the Department of Information Technology, Government of Jharkhand states that pursuant to the UIDAI's Circular and as per Section 29(1) of the Aadhaar Act, the Registrar Packets with JAP-IT, kept on behalf of Department of IT, Government of Jharkhand has been destroyed in presence of a UIDAI team.
178. The Government of Himachal Pradesh has also issued a Certificate dated 09.05.2017 that all Registrar Packets have been destroyed and that no further Registrar Packet is available anywhere with the Registrar. It is also stated that the key for the Registrar Packet has been handed over to respective UIDAI Regional Office team.

179. A Certificate dated 09.05.2017 by the Department of Food, Civil Supplies and Consumer Affairs, Punjab cum Registrar UID, Punjab has certified the destruction of available Registrar Packets and that no further Registrar Packets are available anywhere with the Registrar. The Keys to the Registrar Packet has also been handed over to the UIDAI Regional office team.
180. The Letter dated 06.05.2017 issued by the State Bank of India certifies that no Registrar Packets are available with the State Bank of India for destruction.
181. The Government of Rajasthan has issued a Certificate dated 19.04.2017 certifying that the State Registrar has destroyed all Registrar Packets along with Private Keys and that it is not holding any copy of such packets as well.
182. The Government of Goa has also issued a Certificate dated 04.05.2017 certifying the destruction of all Registrar Packet and that no further Registrar Packet is available anywhere with the Registrar.
183. The Collectorate, Daman as UIDAI Registrar has issued a Certificate dated 05.05.2017 certifying that no Registrar Packet is available with the Registrar and that the key for Registrar Packet has been handed over to the respective UIDAI regional office team.
184. The Central Bank of India by its letter dated 30.05.2017 has confirmed that it does not have any Registrar Packet with it. Likewise, Bank of Baroda vide its Certificate dated 24.05.2017 has also confirmed that it is not holding any packets, particularly Biometrics and other identity information which were collected as part of Aadhaar Enrollment.

185. The Union Bank in its letter dated 26.05.2017 has confirmed that all the Registrar Packets have been destroyed in presence of the UIDAI Regional Office team and that no Registrar Packet is available with them.
186. The Bank of Maharashtra vide Certificate dated 18.05.2017 has confirmed that it is not holding any Registrar Packet particularly Biometrics and other Identity information which were collected as part of Aadhaar Enrollment.
187. A Certificate dated 09.05.2017 by the NSDL E-Governance Infrastructure Limited certifies that it has destroyed all the Registrar Packets available and that no further Registrar Packet is available anywhere with the Registrar.
188. The Government of Gujarat by way of a Certificate dated 09.05.2017 has confirmed the destruction of all Registrar Packets and no Registrar Packet is available anywhere with the Registrar. Further the Key for the Registrar Packet has been destroyed.
189. The Government of Tripura by way of Certificate dated 04.08.2017 has certified that they have destroyed all the Registrar Packets in presence of a team of UIDAI officials and that no Registrar Packets are available anywhere with the Registrar. Further, The Key for the Registrar Packet has also been handed over to the UIDAI Regional Office Team.
190. The contents of para cxxviii and cxxix are completely denied as baseless and incorrect and completely unsubstantiated. The issues are no longer res integra and were examined threadbare before the

Supreme Court. The submissions pertaining to the security measures and technology safeguards in the preceding paragraphs are adopted as a reply to these paragraphs.

B-Data Protection Duties Under The Law-

191. In reply to the contentions of the Petitioner under the heading “B-Data Protection Duties Under the Law”, it is respectfully submitted that there have been no cases of breach of privacy and security of the Aadhaar biometric data in possession of UIDAI. However, UIDAI is conscious of the ever changing technology and the inherent potential risks and has put in place mechanisms to deal with them, which are as follows-

- a. Security and privacy of resident data: Aadhaar by design ensures security and privacy of residents’ data collected through enrolment process. Access to authentication services are given only to authorized ecosystem partners of UIDAI. Under no scenario, biometric data of residents is shared.
- b. Risk to privacy and security of residents’ demographic and biometric data: UIDAI has deployed robust security infrastructure to prevent any unauthorized dissemination of demographic or biometric data of residents stored in central identities data repository (CIDR). Biometric data is never shared with any entity or individuals.

Thus, privacy and security of resident data have been the focus of the UIDAI’s approach since the initiation of the project and the same have been built by design. Hence for Aadhaar, the operations principle has always been – purpose specification, collection limitation, data minimization use,

retention, and disclosure limitation. Aadhaar data cannot be shared by any individual or entity with any individual or entity without the consent of the resident for that particular purpose. Similarly, the Aadhaar number of an individual shall not be published, displayed or posted publicly by any person or entity or agency. Protection of resident data by ensuring confidentiality and privacy is paramount, as per the provisions of the Aadhaar Act. A holistic reading of Section 28 provides that the Authority (UIDAI) shall ensure that the information in the possession or control of the Authority including the information stored in the CIDR is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder and against accidental or intentional destruction, loss or damage. Also, it is very important to note that the resident consent is an underlying feature in the entire process, right from the time of enrolment to the usage of the authentication records. The same has been enshrined in the relevant provisions of the Aadhaar Act as under:

- a. Informed Consent/Disclosure at the time of enrolment as to the manner in which the information collected shall be shared, the nature of recipients with whom the information is intended to be shared during authentication and the existence of the right to access information (Section 3(2)).
- b. Consent of the Aadhaar number holder to be obtained at the time of authentication before collecting personal identity information and a responsibility is cast on the requesting entity to ensure that collected personal identity information is only used for performing authentication. Further, information as to the nature of information that may be shared upon authentication, the uses to which the information

received during authentication be put to use by the requesting entity and alternatives to submission of identity information, shall have to be disclosed to the Aadhaar number Holder during authentication. (Section 8 (2), (3))

- c. Further, Section 29 (3) of the Act, prohibits use of identity information for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication. As such, Aadhaar of an individual can be used for establishing his identity and authentication only with the prior consent of the individual.
- d. Regarding use of information received from Aadhaar through e KYC, it may be noted that while Section 29 (a) and (b) specifically restricts sharing of information for any purpose other than that specified to the individual at the time of submitting identity information, Section 29(4) provides that no Aadhaar number or core biometric information collected or created in respect of an Aadhaar number holder shall be published, displayed or posted publicly.
- e. Disclosure of Identity Information can be made only pursuant to an order of a court not inferior to that of a District Judge (except core biometrics) or disclosure made in the interest of national security in pursuance of a direction of an officer not below the rank of a Joint Secretary to the Government of India specially authorized for the said purpose. Further, any direction issued pursuant to concerns of national security which shall be subject to review an Oversight Committee. (Section 33). This provision has been recommended by the Supreme Court to be partly amended to ensure that the decision is taken at the highest level of the Secretary instead of a Joint Secretary.

125

- f. Contravention of any provisions of the Act would attract penalties as specifically provided for under the Act. (Chapter VII)
 - g. Penalties and Offences: The Act lays down monetary penalties and imprisonment for unauthorized sharing of residents' identity information, failure to keep eKYC data secure, failure to properly inform the residents about the use of their information, or failure to obtain their consent for authentication. The non-compliant individuals or entities may receive monetary penalty (up to one lakh rupees) and/or jail term (up to 3 years) which may vary depending upon the severity and impact of the violation.
 - h. Additionally Aadhaar (Enrolment and update) regulations, Aadhaar (Authentication) Regulations, Aadhaar (Data Security) Regulations, Aadhaar (Data Security) regulations and Aadhaar (Sharing of Information) regulations have specified the manner in which the resident information shall be protected. Thus, UIDAI, has kept the basic principles to protect the privacy of individuals in mind while designing the systems and the Aadhaar Act and the Regulations made thereunder have made that task of ensuring security and privacy easier by embracing data security and privacy principles.
192. It is further submitted that UIDAI has introduced additional features in the form of Virtual ID (VID) service vide Circular No. 1 of 2018, dated 10.01.18 bearing F. No. K-11020/217/2018-UIDAI (Auth-I) issued by the UIDAI. The said circular, issued by UIDAI under the Ministry of Electronics and Information Technology, Government of India provides that with the introduction of Virtual ID, which is a fungible number mapped to an Aadhaar number, Aadhaar number

126

holders have an option not to share their Aadhaar number to further improve privacy. Virtual IDs allow Aadhaar number holders to share the Virtual ID instead of their Aadhaar number during authentication thus reducing the collection of Aadhaar numbers by various agencies. A Virtual ID can only be generated by the Aadhaar number holder. They can also replace (revoke and generate a new one) their Virtual ID from time to time after a minimum validity period set by the UIDAI. Further, UIDAI has also provided various options to Aadhaar number holders to generate their Virtual ID, retrieve it in case they forget their Virtual ID number and also replace their Virtual ID with a new number. These options have been made available with the UIDAI's resident portal, Aadhaar Enrolment Centres, mAadhaar mobile applications etc.

193. This, in light of the above, it is submitted that UIDAI is constantly striving to use innovative and latest technology to ensure data security and privacy of resident data.

C-Appointment of Investigative/Audit Committee-

194. In response to the contentions under the heading (C)-Appointment of Investigative/Audit Committee, it is respectfully submitted that there is no need for the appointment of such a committee as there are already several security committees comprised of highly qualified technology experts in India overseeing the security measures of UIDAI. UIDAI has defined robust security measures to ensure regular audits and reviews of the security deployed at CIDR. Security audits of CIDR are conducted by both internal and external agencies.

127

Internal Agencies-

- a. Internal Security audit done by UIDAI: UIDAI conducts periodic internal audits of the UIDAI CIDR and data centre. The same are headed by UIDAI CISO.
- b. Audits by Managed Service Provider (MSP): There is dedicated security staff from MSP (Managed Service Provider) to implement the various security processes and technology, to ensure security of CIDR and ensure all the processes and systems are running in accordance with the Information Security policy and processes as well as Aadhaar Act and regulations.
- c. Security monitoring agency: UIDAI has also appointed GRCP-SP (Governance, Risk, Compliance, Performance Service Provider) to perform periodic monitoring of the security of internal and external ecosystem.
- External Agency : ISO 27001 certification and Audit by Standardisation Testing & Quality Certification (STQC): UIDAI CIDR is ISO27001:2013 certified since 2015 and goes through yearly surveillance audits from STQC.

D.Constitutional/Common Law Rights And Damages-

195. It is submitted that, in light of the above facts and submissions, the Petitioner has not been able to demonstrate either any legal injury which warrants any compensation nor has the Petitioner been able to demonstrate any breach of the provisions of the Act. In fact, the prayer for damages is in itself a ground for dismissal of the present writ petition wherein the petitioner has an alternative efficacious remedy in

120

a suit for damages. Moreover, disputed questions of facts are involved in this case which cannot be adjudicated by way of exchange of affidavits in writ proceedings and parties would have to lead evidence, the onus to prove the allegations contained in the writ petition would squarely fall on the party making the allegations and therefore, the present writ petition is not an appropriate remedy.

196. The contents of Paragraphs cl to cxcviii are strongly denied as false and completely misplaced. At the outset it is submitted that the Supreme Court in the Aadhaar judgement has categorically rejected the arguments that the Aadhaar project or technology can lead to any kind of surveillance. The Supreme Court after examining the entirety of the project including the technology and after reading down certain provisions like Section 57, has come to the conclusion that the Aadhaar Act as it stands today does not violate privacy and cannot be used for surveillance. The petitioner's argument that being a Muslim and a member of the minority community, he fears that unrestrained access to his data could have potentially fatal implications are nothing but misplaced apprehensions which ought to be rejected as completely baseless borne out of paranoia without any substance or material to show how any data has been used against any person from the minority community or to their detriment. The submissions made in the said paragraphs are completely contrary to the decision of a Constitution bench of the Supreme Court in the Aadhaar judgement which has categorically held that the Aadhaar Act as it stands after the judgement cannot be said to breach privacy or lead to any kind of surveillance. The Act itself prohibits sharing of information with other entities

without the consent of the Aadhaar number holder and it also completely prohibits sharing of any biometric information, making them punishable offences if committed by any person whatsoever. Reasonable and strong safeguards in the form of statutory provisions as well as the technology safeguards are available to protect the data and the apprehensions of the petitioner that being a person from the minority community he is more vulnerable than others is nothing but a figment of the petitioner's feverish imagination.

197. In reply to the contention that the "adjudicating officer" under Section 46 of the IT Act is constitutionally incompetent to adjudicate upon such matters, it is denied as incorrect. It is submitted that the Petitioner has failed to consider that quasi judicial functions are performed by designated officers of various Departments under various laws and the same has been upheld by the Supreme Court. Merely because a person is part of the Department does not render the person constitutionally incapable of discharging its quasi judicial functions. The Petitioner's submission is untenable. If the Petitioner's submissions are accepted, then no departmental officer will be able to perform any quasi judicial functions and all such functions will have to necessarily be outsourced to so called independent persons.

198. In reply to the contentions under sub heading "D.3 –Common Law Remedies", it is humbly submitted that the Petitioner is not entitled to any common law remedy because he has failed to show how he has suffered any injury on account of the acts or omissions of the Respondent herein.

199. Firstly, the allegation of negligence on part of the Respondent herein is an unfounded claim based on certain media reports, and as stated earlier, Respondent has already taken action in appropriate cases. Respondent humbly submits that in order to prove tortious liability, Petitioner has to first prove that he has suffered some legal injury. In a case where the occurrence of the event of security breach is itself false, there is no question of a claim for damages under torts to be paid to the Petitioner. Petitioner's claim for damages in tort ought to be claimed in an appropriate suit after leading evidence rather than in a writ proceeding.
200. Secondly, regarding the contentions under the sub-heading D.3.2.2- Misuse of Private Information and Damages, it is humbly submitted that the very basis of this contention, i.e. publication of personal data of Aadhaar holders is a fictitious claim and therefore Petitioner cannot claim damages based on such unsubstantiated claims.
201. It is humbly submitted that the case law relied upon by the Petitioner is not applicable to the present case because there has been no data breach in the present case, contrary to the assertion made by the Petitioner.
202. With regard to the allegation that Petitioner has been receiving unsolicited e-mails, texts etc., it is humbly submitted that in the wake of the Aadhaar judgment doing away with the requirement of linking the Aadhaar number to bank account, mobile etc., this grievance of Petitioner is already taken care of and the claim has become infructuous.
203. As far as the contention under the sub heading D.4- Constitutional Torts is concerned, it is humbly submitted that the averments made

therein stand answered by the judgment of the Hon'ble Supreme Court vide the Aadhaar judgment wherein the Hon'ble Supreme Court has upheld the constitutional validity of Aadhaar Act by reading down certain provisions of the Aadhaar Act and while doing so, the Hon'ble Court has held that the Aadhaar Act does not violate right to privacy enshrined under Article 21. Therefore, in the absence of violation of any constitutional rights of the Petitioner, he cannot set up a case for constitutional tort or claim damages for it.

E. Right to Know-

204. Petitioner claims that his right to know of the security practices pertaining to Aadhaar data and of any breaches of the Aadhaar database. The said contention is vehemently denied by the Respondent, in light of the submissions made in the paragraphs above of the present Affidavit.
205. As far as the contention regarding Section 8(1) of the Right to Information Act and Annexure P-25 is concerned, it is humbly submitted that the UIDAI's Central Identities Data Repository (CIDR) in which the data is stored has been declared as "Protected System" under Section 70 of the Information Technology Act, 2000 whereby the government can declare any computer resource, which directly or indirectly affects the facility of critical information infrastructure to be a protected system. The Explanation to Sec. 70 defines Critical Information Infrastructure to mean the computer resource, the **incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety.** Section 70 (3) states that any person who secures access or attempts to

132

secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment upto 10 years and will also be liable to fine. In light of the CIDR having been declared as a protected system being a critical information infrastructure, and in light of the Explanation to Section 70, the exemption under Section 8(1)(a) of the RTI Act would squarely apply wherein exemption from disclosure of information has been provided with respect to "information, disclosure of which would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State". Relevant extract of Section 8 is as follows:

8. Exemption from disclosure of information.—

(1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,—

(a) information, disclosure of which would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State, relation with foreign State or lead to incitement of an offence;

In addition to the above, it is humbly submitted that every allegation of breach has been enquired into, investigated and press releases made. The UIDAI has consistently maintained that there has not been a single breach of the CIDR. The reason for non-disclosure of security information or the minutae of the security policies is quite obvious and any request for such disclosure which may jeopardise the security of the data of over a billion people can be denied in larger public interest which is consistent even with the RTI Act itself. Therefore the contentions of Petitioner in this regard is completely misplaced and untenable.

133

F. Right to Legal Redressal-

206. The grievance regarding Section 47(1) of the Act already stands answered by the Hon'ble Supreme Court in Aadhaar judgment under paragraph No. 449 (4) (g) of the judgment-

“(g) Insofar as Section 47 of the Act which provides for the cognizance of offence only on a complaint made by the Authority or any officer or person authorised by it is concerned, it needs a suitable amendment to include the provision for filing of such a complaint by an individual/victim as well whose right is violated.”

Therefore, the request for a neutral ombudsman in the interim need no longer be gone into since the Hon'ble Supreme Court has already given its ruling on the issue of Section 47.

Reply to the Grounds for Relief-

207. That it is humbly submitted that the present Writ Petition does not raise any tenable grounds and the grounds raised therein merit rejection. Therefore, it is most respectfully submitted that the present Petition should be dismissed as it does not raise any ground for the interference of this Hon'ble Court. The Respondent herein seeks to refer to and rely upon the submissions made hereinabove in reply to the grounds raised by the Petitioner and is not repeating those submissions in order to avoid prolixity.

Prayer-

134

208. That in reply to the Prayer made by the Petitioner, it is humbly submitted that the same deserves to be rejected as the Petitioner has failed to establish any grounds for grant of the relief prayed for.

209. In view of the above submissions, the present Writ Petition deserves to be dismissed with costs.


DEPONENT

क्षेत्रीय कार्यालय, दिल्ली/Regional Office, Delhi
भारतीय विशिष्ट पहचान प्राधिकार
Unique Identification Authority of India
भारत सरकार/Government of India
इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय,
Ministry of Electronics & Information Technology

VERIFICATION:-

Verified at New Delhi on the day of 12th February 2019 that the averments and submissions made above are true to the best of my knowledge, which is based on the records of the case which are under my charge and nothing material has been concealed there from.


DEPONENT

रमेश कुमार/Ramesh Kumar
उप निदेशक/Deputy Director
क्षेत्रीय कार्यालय, दिल्ली/Regional Office, Delhi
भारतीय विशिष्ट पहचान प्राधिकार
Unique Identification Authority of India
भारत सरकार/Government of India
इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय,
Ministry of Electronics & Information Technology

Through

New Delhi
Dated:12/02/2019

(Zohab Hossain)
Advocate for Respondent No. 1
S-74, LGF, Greater Kailash Part 1,
New Delhi – 110 048
M. 9999711099
E: hossainzohab@gmail.com

THE SUPREME COURT OF INDIA
CIVIL ORIGINAL JURISDICTION
WRIT PETITION (C) NO. 797 OF 2016

135
Annexure R - 1

IN THE MATTER OF:

S.G. Vombatkere & Anr.

..Petitioner

Versus

Union of India & Ors.

...Respondents

WITH

ADDITIONAL AFFIDAVIT

PAPER BOOK

(FOR INDEX : PLEASE SEE INSIDE)

ADVOCATES FOR THE PETITIONER: M/S. K.J. JOHN & CO.

INDEX

136

<u>SL.NO.</u>	<u>PARTICULARS</u>	<u>PAGE(S)</u>
1.	Additional Affidavit of Petitioner No.2.	1-5
2.	<u>ANNEXURE- A/1</u> Copy of Affidavit dated 18.11.2017 of one Mr. C.A. Fernandes of Mangalore,	6-15
3.	<u>ANNEXURE- A/2</u> Copy of the Affidavit of Mr. Siraj Dutta dated 06.01.2018	16-51
4.	<u>ANNEXURE- A/3</u> Copy of the Affidavit of Dr. Yogesh Jain, a medical practitioner dated 09.01.2018	52-60
5.	<u>ANNEXURE- A/4</u> Copy of the case study referred to in the Affidavit of Dr. Yogesh Jain.	61-64
6.	<u>ANNEXURE- A/5</u> Copy of the Fact Finding Report undertaken by Mr. Narasimhappa, member of the Bangalore-People's Union for Civil Liberties dated 29.07.2017.	65-71
7.	<u>ANNEXURE- A/6</u> Copy of the paper titled "Impact of Biometrics in India" by Dr. S. Ananth in the Staff Paper Series dated October 2017 of the RBI-backed Institute for Development and Research in Banking Technology (IDRBT).	72-103
8.	<u>ANNEXURE- A/7</u> Copy of the News Report titled "Less than 50 percent HIV patients link Aadhaar to Anti-Retroviral Therapy services- The New Indian Express" as it appeared in the New Indian Express on 03.01.2018.	104-105

9. **ANNEXURE- A/8**

Copy of the News Report titled "Uttarakhand: No Aadhaar: 53,000 denied pension in Uttarakhand" as it appeared in the Times of India on 09.01.2018.

106-107

137

10. **ANNEXURE- A/9**

Copy of the News Report titled "Kargil widow dies, son says hospital wanted Aadhaar card to start treatment" as published on 31.12.2017 in the Indian Express.

108-110

11. **ANNEXURE- A/10**

Copy of the News Report as published in the news web portal TheWire.in dated 15.11.2017 and titled "Woman in Bareilly Reportedly Dies of Starvation After Husband Was Denied Ration".

111-112

12. **ANNEXURE- A/11**

Copy of the News Report as published in The Tribune, a Chandigarh based news daily, titled "Rs 500, 10 minutes, and you have access to billion Aadhaar details" as published on 04.01.2018.

113-116

13. **ANNEXURE- A/12**

Copy of the First Information Report filed by the UIDAI following the aforementioned news report in The Tribune.

117-120

14. **ANNEXURE- A/13**

Copy of the affidavit dated 08.01.2018 of Shri Sanjeev concerning exclusion of persons effected by Leprosy from legal entitlements due to Aadhar.

121-135

138

tribuneindia.com

Rs 500, 10 minutes, and you have access to billion Aadhaar details

Tribune News Service

7-8 minutes

Nation

Posted at: Jan 4, 2018, 2:07 AM; last updated: Jan 5, 2018, 1:58

PM (IST) TRIBUNE INVESTIGATION — SECURITY

BREACH Group tapping UIDAI data may have sold access to 1 lakh service providers



Rachna Khaira

Tribune News Service

Jalandhar, January 3

139

It was only last November that the UIDAI asserted that "Aadhaar data is fully safe and secure and there has been no data leak or breach at UIDAI." Today, The Tribune "purchased" a service being offered by anonymous sellers over WhatsApp that provided unrestricted access to details for any of the more than 1 billion Aadhaar numbers created in India thus far. (Follow [The Tribune on Facebook](#); and [Twitter @thetribunechd](#)) It took just Rs 500, paid through Paytm, and 10 minutes in which an "agent" of the group running the racket created a "gateway" for this correspondent and gave a login ID and password. Lo and behold, you could enter any Aadhaar number in the portal, and instantly get all particulars that an individual may have submitted to the UIDAI (Unique Identification Authority of India), including name, address, postal code (PIN), photo, phone number and email. What is more, The Tribune team paid another Rs 300, for which the agent provided "software" that could facilitate the printing of the Aadhaar card after entering the Aadhaar number of any individual. When contacted, UIDAI officials in Chandigarh expressed shock over the full data being accessed, and admitted it seemed to be a major national security breach. They immediately took up the matter with the UIDAI technical consultants in Bangaluru. Sanjay Jindal, Additional DirectorGeneral, UIDAI Regional Centre, Chandigarh, accepting that this was a lapse, told The Tribune: "Except the Director-General and I, no third person in Punjab should have a login access to our official portal. Anyone else having access is illegal, and is a major national security breach." 1 lakh illegal users

Investigations by The Tribune reveal that the racket may have started around six months ago, when some anonymous groups were created on WhatsApp. These groups targeted over 3 lakh village-level enterprise (VLE) operators hired by the Ministry of Electronics and Information Technology (ME&IT) under the Common Service Centres Scheme (CSCS) across India, offering them access to UIDAI data. CSCS

146

operators, who were initially entrusted with the task of making Aadhaar cards across India, were rendered idle after the job was withdrawn from them. The service was restricted to post offices and designated banks to avoid any security breach in November last year. Spotting an opportunity to make a quick buck, more than one lakh VLEs are now suspected to have gained this illegal access to UIDAI data to provide "Aadhaar services" to common people for a charge, including the printing of Aadhaar cards. However, in wrong hands, this access could provide an opportunity for gross misuse of the data. The hackers seemed to have gained access to the website of the Government of Rajasthan, as the "software" provided access to "aadhaar.rajasthan.gov.in", through which one could access and print Aadhaar cards of any Indian citizen. However, it could not be ascertained whether the "portals" were genuinely of Rajasthan, or it was mentioned just to mislead. Sanjay Jindal said all of this could be confirmed only after a technical investigation was conducted by the UIDAI.

'Privacy at risk' "Leakage of Aadhaar data reveals that the project has failed the privacy test. At the recently concluded 11th WTO Ministerial Conference, India submitted a written position on e-commerce, opposing the demand for negotiations on e-commerce by the US and its allies. The latter were demanding access to citizens' database for free. The revelation by The Tribune also means that the proposed data protection law will now hold no purpose, as the data has already been breached. The state governments must immediately disassociate themselves and cancel the MoU signed with UIDAI," said Gopal Krishan, New Delhi-based convener of the Citizens Forum for Civil Liberties, who appeared before the Special Parliamentary Committee that examined the Aadhaar Bill in 2010. A quick chat, and full access

141

12:30 pm: This correspondent posing as 'Anamika' contacted a person on WhatsApp number 7610063464, who introduced himself as 'Anil Kumar'. He was asked to create an access portal.

12:32pm: Kumar asked for a name, email ID and mobile number, and also asked for Rs 500 to be credited in his Paytm No. 7610063464.

12:35 pm: This correspondent created an email ID, aadharjalandhar@gmail.com, and sent mobile number *****5852 to the anonymous agent.

12:48 pm: Rs 500 transferred through Paytm.

12:49 pm: This correspondent received an email saying, "You have been enrolled as Enrolment Agency Administrator for 'CSC SPV'. Your Enrolment Agency Administrator ID is 'Anamika_6677'." Also, it was said that a password would be sent in a separate mail, which followed shortly.

12:50 pm: This correspondent had access to the Aadhaar details of every Indian citizen registered with the UIDAI.

Printing Aadhaar card This correspondent later again approached Anil Kumar to ask for software to print Aadhaar cards. He asked for Rs 300 through Paytm No. 8107888008 (in the name of 'Raj'). Once paid, a person identifying himself as Sunil Kumar called from mobile number 7976243548, and installed software on this correspondent's computer by accessing it remotely through "TeamViewer". Once the job was done, he deleted the software drivers, even from the recycle bin.

Possible misuse Getting SIM cards, or bank accounts in anyone's name. Last month, a man was arrested in Jalandhar for withdrawing money from someone's bank account by submitting a fake Aadhaar card.

7719

(पृष्ठ 154 के परिच्छेद नवम - १०५५)

$\varphi(\alpha)$	Section($\text{SPR}(\alpha)$)
$\sigma(\alpha)$	$\text{SPR}(\text{ZUS}(\alpha))$

592

No.	Property Type(Description)	Est. Value(Rs.)	Status
1	...	...	...

attach separate sheet, if required (use extra sheet only)

(attach separate sheet, if required) (Date: 08/01/2019)

Department of India Ministry of Electronics & Information Technology Unique Identification Number Authority
India Regional office, Chandigarh To-Mr Sandeep Lamba, ACP, Cyber Cell Crime Branch
Assistant Commissioner of Police, Old Kotwali Building Daryaganj Delhi-110002 Complainant
Kumar, Sunil Kumar, Raj, Rachna Khaira, The Tribune and other unknown persons are
is of Section 36 and 37 of the Aadhaar Act, 2016, Section 419, 420, 468 and 471 of
Section 66 of IT Act, 2000. Sir, An input has been received through Newspaper
dated 3rd January, 2018 that "The Tribune" purchased a service being offered by anonymous
number created in India thus far." The relevant four page extract of the newspaper downlink
www.tribuneindia.com/news/nation and the newspaper clipping are enclosed herewith. It is
mentioned in this newspaper that "a correspondent of The Tribune posing as 'Anamika' contacted
a WhatsApp number 7610063464, who introduced himself as 'Anil Kumar'. He was asked
for access portal. Thereafter, Anil Kumar asked for a name, email ID and mobile number, an
amount of Rs. 500 to be credited in his Paytm No. 7610063464. Thereafter, The Tribune
created an email ID, aadharjalandnar@gmail.com, and sent mobile number *****5652.
Anonymous agent and transferred Rs. 500 through Paytm. It has thereafter been stated that the
correspondent received an email saying, "You have been enrolled as Enrolment Agency Administrator for 'CSC SPV'. Your Enrolment Agency Administrator ID is 'Anamika_6577' and that a
word would be sent in a separate mail, which followed shortly." It has further been alleged in the
newspaper clipping that The Tribune correspondent had access to the Aadhaar details of every
citizen registered with the UIDAI. Further, it has been alleged through this newspaper that the
correspondent again approached Mr. Anil Kumar for software to print Aadhaar cards for which Mr. Anil
asked for Rs. 300 through Paytm No. 6107888008 (in the name of 'Raj'). Once paid, a person
posing himself as Sunil Kumar called from mobile number 7975243548, and installed software on
correspondent's computer by accessing it remotely through "Team Viewer". The above mentioned
persons have unauthorisedly accessed the Aadhaar eco system in connivance of the crime
agency. The above act of the aforesaid involved persons namely Anil Kumar, Sunil Kumar, Raj,
Rachna Khaira, The Tribune and other unknown persons is violations of Section 36 and 37 of
Aadhaar Act, 2016 Section 419, 420, 468 and 471 of IPC 1860 and Section 66, IT Act, 2000. An input
received dated 03/01/2018 was done by UIDAI office and it has come to the notice that above violations
under the Grievance Redressal System of UIDAI situated at 9th floor, Tower-1, UIDAI
Building, New Delhi and hence, FIR needs to be filed at Cyber Cell, Crime Branch,
Chandigarh. From the content of the complaint and attached was clippings, prima facie
case against persons under Section 36 and 37 of the Aadhaar (Targeted delivery of
financial and other subsidies, benefits and services) Act, 2016, Section 419, 420, 468 and 471 of
IPC and Section 66 of IT Act, 2000 has been made out. B.M. Pattnaik DD (Logistics and
Complaints), CID, Chandigarh. Copy of the complaint and attached was clippings, prima facie
case against persons under Section 36 and 37 of the Aadhaar (Targeted delivery of
financial and other subsidies, benefits and services) Act, 2016, Section 419, 420, 468 and 471 of
IPC and Section 66 of IT Act, 2000 has been made out. B.M. Pattnaik DD (Logistics and
Complaints), CID, Chandigarh.

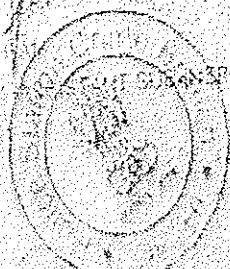
119

2002-2003

DATE: 11/27/1968
 TO: DIRECTOR, FBI
 FROM: SAC, NEW YORK (100-100000)
 SUBJECT: [REDACTED]

Signature of Officer _____

RECEIVED
JAN 19 1964
U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250



10-11-68 (10-11-68)

Received 08-12/18
at 2:00 AM
12/18

145
Annexure R-2

IN THE SUPREME COURT OF INDIA
CIVIL ORIGINAL JURISDICTION

IA NO. OF 2018

IN

WRIT PETITION (CIVIL) NO. 1056 OF 2017

Nachiket Udupa & Another

... PETITIONERS

VERSUS

Union of India & Others

... RESPONDENTS

AN APPLICATION SEEKING PERMISSION TO PLACE
CERTAIN ADDITIONAL DOCUMENTS ON RECORD

PAPERBOOK
(KINDLY SEE INSIDE FOR INDEX)

T. V. S. RAGHAVENDRA SREYAS
ADVOCATE FOR PETITIONERS

146

INDEX

S. No.	Particulars	Page Nos.
1.	I.A. No. of 2018: An application seeking permission to place certain additional documents along with affidavit	1 – 7
2.	ANNEXURE A-1: True copy of “Privacy Policy Guidance Memorandum”, Memorandum Number 2007-02 released by US Department of Homeland Security, Washington DC on 04.06.2007	8 – 11
3.	ANNEXURE A-2: True copy of relevant extracts from the Planning Commission, Government of India, “Report of the Group of Experts on Privacy” dated 16.10.2012	12 – 30
4.	ANNEXURE A-3: True copy of relevant extracts from the Report by the Whither Biometrics Committee, National Research Council of the National Academies, Division on Engineering and Physical Science on “Biometric Recognition: Challenges and Opportunities” (2010, Washington DC)	31 – 58
5.	ANNEXURE A-4: True copy of article by Anumeha Yadav, “In Rajasthan, there is ‘unrest at the ration shop’ because of error-ridden Aadhaar” dated 02.04.2016	59 – 66
6.	ANNEXURE A-5: True copy of Reply of the Minister of Finance dated 09.08.2016 to Unstarred Question No. 2556 in the Rajya Sabha on “Technical problems faced in subsidy transfers”	67 – 68
7.	ANNEXURE A-6: True copy of Notification u/s. 7 of the Aadhaar Act issued by Ministry of Consumer Affairs, Food & Public Distribution on 08.02.2017	69 – 72

147

8. ANNEXURE A-7: True copy of article 73 – 79
authored by Anmol Somanchi *et al*, “Well Done ABBA?: Aadhaar and the Public Distribution System in Hyderabad”, 52(7) *Economic and Political Weekly* dated 18.02.2017
9. ANNEXURE A-8: True copy of Press 80
Release dated 27.03.2017 issued by Government of Jharkhand
10. ANNEXURE A-9: True copy of Article 81 – 103
authored by Shweta Agrawal *et al*, “Privacy and Security of Aadhaar: A Computer Science Perspective”, 52(37) *Economic and Political Weekly* dated 16.09.2017
11. ANNEXURE A-10: True copy of CBSE 104 – 105
notification, CBSE/ASC/Reg/112510/2018 dated 26.09.2017 making Aadhaar mandatory for online registration of Class IX/XI students for 2017/18
12. ANNEXURE A-11: True copy of article in 106 – 109
the *Scroll.in* by Jean Dreze, “*Chronicle of a starvation death foretold: Why it is time to abandon Aadhaar in the ration shop*” dated 21.10.2017
13. ANNEXURE A-12: True copy of Article 110 – 119
authored by Jean Dreze *et al*, “Aadhaar and Food Security in Jharkhand: Pain Without Gain?”, 52(50) *Economic & Political Weekly* dated 16.12.2017
14. ANNEXURE A-13: True copy of article in 120
The New Indian Express, “*No fingers or iris for Aadhaar, Bengaluru woman loses pension*” dated 02.12.2017
15. ANNEXURE A-14: True copy of Reply of 121 - 123
the Minister of Electronics and Information Technology dated 20.12.2017 to Unstarred Question No. 819 in the Lok Sabha on

148

"Mandatory Aadhaar Linkage"

16. ANNEXURE A-15: True copy of Reply of the Minister of Consumer Affairs, Food and Public Distribution dated 02.01.2018 to Unstarred Question No. 2477 in the Lok Sabha on "Availing Aadhaar" 124
17. ANNEXURE A-16: True copy of Reply of the Minister of Electronics and Information Technology dated 03.01.2018 to Unstarred Question No. 2582 in the Lok Sabha on "Breach of Aadhaar Data" 125
18. ANNEXURE A-17: True copy of Reply of the Minister of Electronics and Information Technology dated 03.01.2018 to Unstarred Question No. 2759 in the Lok Sabha on "Memorandum of Citizens Regarding Aadhaar" 126
19. ANNEXURE A-18: True copy of the News Reports as published in The Tribune, a Chandigarh based news daily, titled "*Rs 500, 10 minutes, and you have access to billion Aadhaar details*" and UIDAI denies any breach of Aadhaar data" as published on 04.01.2018 127 - 132
20. ANNEXURE A-19: True copy of UIDAI's FAQ page 133

149

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2582
TO BE ANSWERED ON 03-01-2018

BREACH OF AADHAAR DATA

2582. **SHRI AJAY MISRA TENI:**
SHRI J.C. DIVAKAR REDDY:
SHRIMATI KOTHAPALLI GEETHA:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that names and addresses of some Aadhaar cardholders were made public on more than 200 websites of Central and State Governments as per Unique Identification Authority of India (UIDAI);

(b) if so, the details thereof;

(c) the action taken by the Government against the departments of Central and State Government and education institutes and private organisations who have made the names and address of Aadhaar cardholders public;

(d) whether any steps have been taken by the Government to ensure that the information of Aadhaar cardholders is not made public by any Government and private department; and

(e) if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION
TECHNOLOGY
(SHRI ALPHONS KANNANTHANAM)

(a) and (b): Yes, Sir. It was found that approximately 210 websites of Central Government, State Government departments and some educational institutes were displaying the list of beneficiaries along with their name, address, other details and Aadhaar numbers for information of general public.

(c) to (e): The concerned departments/websites were instructed to remove the Aadhaar and other personal data from the said websites. In addition, the Central and State Governments have been advised to sensitize all Ministries/ Departments to take all precautions while publishing or sharing data on their websites and ensure compliance of Aadhaar Act, 2016 and Information Technology Act, 2000.

150

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2759
TO BE ANSWERED ON 03-01-2018

MEMORANDUM FROM CITIZENS REGARDING AADHAAR

2759. SHRI KALIKESH N. SINGH DEO:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether the Government has received any memorandum from citizens asking for their information to be deleted from the Aadhaar database and their Aadhaar cards be cancelled;
- (b) if so, the action taken by the Government in this regard;
- (c) whether a provision has been made for citizens to opt out of the Aadhaar scheme, especially for those not receiving any welfare benefit from the Government;
- (d) if so, the details thereof and if not, the reasons therefor;
- (e) whether fresh consent is sought every time Aadhaar scheme is extended to new schemes, if so, the details thereof and if not, the reasons therefor; and
- (f) whether there is provision to revoke consent from using Aadhaar card for new schemes and if so, the details thereof and if not, the time by which the Government is likely to bring out such a provision?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ALPHONS KANNANTHANAM)

(a) and (b): All the requests received for deactivation or cancellation from citizens are dealt as per Para 27, 28 and 29 of the Aadhaar (Enrolment & Update) Regulations, 2016. Para 27 of the Aadhaar (Enrolment & Update) Regulations, 2016 makes provision for cancellation of Aadhaar.

(c) and (d): No, Sir. There is no provision in the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 for citizens to opt out of the Aadhaar scheme.

(e) and (f): As per Section 8 of the Aadhaar Act, consent of an individual is obtained before collecting his identity information for the purposes of authentication of the Aadhaar number of an Aadhaar number holder. The identity information of an individual is only used for submission to the Central Identities Data Repository (CIDR) for authentication. Besides, under Section 8(3) of the Aadhaar Act, 2016 read with the Regulation 5 and 6 of the Aadhaar (Authentication) Regulation, 2016 of the said Act, the individual submitting his identity information for authentication, shall be informed of the following details with respect to authentication, namely:-

- (i) The nature of information that may be shared upon authentication;
- (ii) The uses to which the information received during authentication may be put; and
- (iii) Alternatives to submission of identity information.

Unique Identification Authority of India (UIDAI) issues Aadhaar numbers and provides authentication services for establishing identity of the beneficiaries. The usage of Aadhaar for delivery of welfare service, benefits or any other purpose and the extent to which Aadhaar is to be used is determined by the implementing agencies such as State Governments/Central Ministries and other agencies. It is upto the citizen to give consent for any scheme.

Thursday, January 11, 2018

The Tribune

VOICE OF THE PEOPLE

facebook

HOME | NATION | WORLD | PUNJAB | HARYANA | HIMACHAL | J & K | UTTARAKHAND | CITIES | OPINION | SPORT | BUSINESS | FEATURES

Nation

Posted at: Jan 4, 2018, 2:07 AM; last updated: Jan 5, 2018, 1:58 PM (IST)

TRIBUNE INVESTIGATION — SECURITY BREACH

Rs 500, 10 minutes, and you have access to billion Aadhaar details

Group tapping UIDAI data may have sold access to 1 lakh service providers



Rachna Khaira
Tribune News Service
Jalandhar, January 3

It was only last November that the UIDAI asserted that "Aadhaar data is fully safe and secure and there has been no data leak or breach at UIDAI." Today, The Tribune "purchased" a service being offered by anonymous sellers over WhatsApp that provided unrestricted access to details for any of the more than 1 billion Aadhaar numbers created in India thus far.

(Follow [The Tribune on Facebook](#); and [Twitter @thetribunechd](#))

It took just Rs 500, paid through Paytm, and 10 minutes in which an "agent" of the group running the racket created a "gateway" for this correspondent and gave a login ID and password. Lo and behold, you could enter any Aadhaar number in the portal, and instantly get all particulars that an individual may have submitted to the UIDAI (Unique Identification Authority of India), including name, address, postal code (PIN), photo, phone number and email.

What is more, The Tribune team paid another Rs 300, for which the agent provided "software" that could facilitate the printing of the Aadhaar card after entering the Aadhaar number of any individual.

When contacted, UIDAI officials in Chandigarh expressed shock over the full data being accessed, and admitted it seemed to be a major national

Related Articles

UIDAI denies any breach of Aadhaar data

Aadhaar data breach finds mention in Parliament

Aadhaar data breach shocks Twitterati, top trend for the day

Also in this section

BJP draws parallel between Siddaramaiah and Hafiz Saeed

Tibetan PM-in-exile cautions India against China

No point in securing Aadhaar data now: Chidambaram

US Ambassador bats for India-US Free Trade Agreement

In London, Rijiju seeks UK help in early extradition of Mallika

TOP STORIES



India, Pak NSAs met in Thailand, 'talks on terror' can go ahead: MEA



Justice Dhingra to supervise probe into 186 anti-Sikh riot cases



Supreme Court to hear plea for probe into CBI judge Loya's death



Nitin Gadkari's earful for naval top brass for 'obstructing development'



Indu Malhotra first woman lawyer to be directly appointed as SC judge

CITY FOCUS

Chandigarh



Woman, daughter put up brave fight

11 Jan 2018 | 1:58 AM

CHANDIGARH: Ritu Jain, a jewellery

designer, who, along with her daughter and servant, was present in the house in Sector 33 when the robbery took place, was injured after she tried to fight the robbers.

Dog bite hurts more as dispensaries sans vaccine

PU Prof dies of cardiac arrest in Rajasthan

GMADA set to offer 900 residential plots

2 women among three held for minor's rape, murder

30-yr-old convicted of widow's rape

Ex-Mayor was controversy's child

Day of bouquets

[more Chandigarh...](#)

SCI/TECH/GADGETS/ENV.



for origin of life on Earth

[more SciTech...](#)

HEALTH



technical consultants in Bangaluru.

Sanjay Jindal, Additional Director-General, UIDAI Regional Centre, Chandigarh, accepting that this was a lapse, told The Tribune: "Except the Director-General and I, no third person in Punjab should have a login access to our official portal. Anyone else having access is illegal, and is a major national security breach."



l in pregnancy may
nters' language skills

more Health...

1 lakh illegal users

Investigations by The Tribune reveal that the racket may have started around six months ago, when some anonymous groups were created on WhatsApp. These groups targeted over 3 lakh village-level enterprise (VLE) operators hired by the Ministry of Electronics and Information Technology (ME&IT) under the Common Service Centres Scheme (CSCS) across India, offering them access to UIDAI data.

CSCS operators, who were initially entrusted with the task of making Aadhaar cards across India, were rendered idle after the job was withdrawn from them. The service was restricted to post offices and designated banks to avoid any security breach in November last year.

Spotting an opportunity to make a quick buck, more than one lakh VLEs are now suspected to have gained this illegal access to UIDAI data to provide "Aadhaar services" to common people for a charge, including the printing of Aadhaar cards. However, in wrong hands, this access could provide an opportunity for gross misuse of the data.

The hackers seemed to have gained access to the website of the Government of Rajasthan, as the "software" provided access to "aadhaar.rajasthan.gov.in", through which one could access and print Aadhaar cards of any Indian citizen. However, it could not be ascertained whether the "portals" were genuinely of Rajasthan, or it was mentioned just to mislead.

Sanjay Jindal said all of this could be confirmed only after a technical investigation was conducted by the UIDAI.

'Privacy at risk'

"Leakage of Aadhaar data reveals that the project has failed the privacy test. At the recently concluded 11th WTO Ministerial Conference, India submitted a written position on e-commerce, opposing the demand for negotiations on e-commerce by the US and its allies. The latter were demanding access to citizens' database for free. The revelation by The Tribune also means that the proposed data protection law will now hold no purpose, as the data has already been breached. The state governments must immediately disassociate themselves and cancel the MoU signed with UIDAI," said Gopal Krishan, New Delhi-based convener of the Citizens Forum for Civil Liberties, who appeared before the Special Parliamentary Committee that examined the Aadhaar Bill in 2010.

A quick chat, and full access

- 12:30 pm: This correspondent posing as 'Anamika' contacted a person on WhatsApp number 7610063464, who introduced himself as 'Anil Kumar'. He was asked to create an access portal.
- 12:32pm: Kumar asked for a name, email ID and mobile number, and also asked for Rs 500 to be credited in his Paytm No. 7610063464.
- 12:35 pm: This correspondent created an email ID, aadharjalandhar@gmail.com, and sent mobile number *****5852 to the anonymous agent.

12:47 pm: The correspondent received an email saying, "You have been enrolled as Enrolment Agency Administrator for 'CSC SPV'. Your Enrolment Agency Administrator ID is 'Anamika_6677'." Also, it was said that a password would be sent in a separate mail, which followed shortly.

- 12:50 pm: This correspondent had access to the Aadhaar details of every Indian citizen registered with the UIDAI.

Printing Aadhaar card

This correspondent later again approached Anil Kumar to ask for software to print Aadhaar cards. He asked for Rs 300 through Paytm No. 8107888008 (in the name of 'Raj'). Once paid, a person identifying himself as Sunil Kumar called from mobile number 7976243548, and installed software on this correspondent's computer by accessing it remotely through "TeamViewer". Once the job was done, he deleted the software drivers, even from the recycle bin.

Possible misuse

Getting SIM cards, or bank accounts in anyone's name. Last month, a man was arrested in Jalandhar for withdrawing money from someone's bank account by submitting a fake Aadhaar card.



Sitaram Yechury
@SitaramYechury

The perils of making Aadhaar mandatory and linking it to bank accounts, as insisted upon by Modi govt, are visible here. Do we need more proof to stop this madness?

tribuneindia.com/news/nation/rs...

9:06 AM - Jan 4, 2018

Rs 500, 10 minutes, and you have access to ...

JALANDHAR:It was only last November that the UIDAI asserted that "Aadhaar data is fully safe and secure and there has been no data leak or
tribuneindia.com

81 646 833



Randeep S Surjewala
@rssurjewala

'AADHAR' data breached yet again!

As every citizen's personal information is exposed to hackers everyday & 'Right to Privacy' is mocked and flouted with impunity, Modi Govt remains immune.

Is anyone listening?
tribuneindia.com/news/nation/rs...

9:29 AM - Jan 4, 2018

Rs 500, 10 minutes, and you have access to ...

JALANDHAR:It was only last November that the UIDAI asserted that "Aadhaar data is fully safe and secure and there has been no data leak or
tribuneindia.com

152 987 2,076

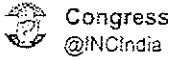


Nitin A. Gokhale
@nitinagokhale

This is dangerous and criminal negligence of data security. Kudos to the reporter for unveiling the racket. A crackdown on the culprits & a corrective step is imperative: Rs 500, 10 minutes, and you have access to billion Aadhaar details
tribuneindia.com/news/nation/rs... via @theTribuneChd

Rs 500, 10 minutes, and you have access to ...
 JALANDHAR:It was only last November that the
 UIDAI asserted that "Aadhaar data is fully safe
 and secure and there has been no data leak or
 tribuneindia.com

11 102 84



Rs 500. That's all it takes for someone to steal the data of a
 billion citizens. Envisioned by UPA as a tool for inclusion,
 #Aadhaar has become an identity theft nightmare under the
 NDA. tribuneindia.com/news/nation/rs..
 10:32 AM - Jan 4, 2018

Rs 500, 10 minutes, and you have access to ...
 JALANDHAR:It was only last November that the
 UIDAI asserted that "Aadhaar data is fully safe
 and secure and there has been no data leak or
 tribuneindia.com

132 950 1,376

COMMENTS

All readers are invited to post comments responsibly. Any messages with foul language or
 inciting hatred will be deleted. Comments with all capital letters will also be deleted.
 Readers are encouraged to flag the comments they feel are inappropriate.
 The views expressed in the Comments section are of the individuals writing the post. The
 Tribune does not endorse or support the views in these posts in any manner.

329 Comments tribuneindia

Login

Recommend 20 Share

Sort by Best



Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name



Raj • 8 days ago

Goldmine for Identity Thiefs..Modi will be Manmohan, Shah will be Firak, Jaitley will
 be Jhuatalia Begum..It will be fun, like old movies anyone can assume any other identity
 with changed photo..BJP RSS Mastermind of Digital Frauds and Loot.. Who got Rs. 15
 Lakh ? ANYONE. Half of Pakistan will have Indian ID and Details..Mast Chor hey BJP
 26 ^ v . Reply . Share



Conscience Killer → Raj • 7 days ago

Don't think the politicians have Aadhaar Cards. These cards are for the common
 people and not for the elites.

9 ^ v . Reply . Share



Raj → Conscience Killer • 7 days ago

Agree or they may have 4 or 5..only one will be authentic and only they
 know it..Crooked BJP RSS..Deed Land Lease all can be just "Flipped" to
 anyone who has the document and like movie Dhoop keep running
 around that "You" are "You"..Mast Majani Life in India

7 ^ v . Reply . Share



Majwa → Raj • 7 days ago

You remember how some in Mumbai stole millions from North
 Americans
 pretending to be from Revenue service, Immigration etc. Most of
 the
 victims were elderly and or immigrants. They use to phone the
 victims with all the information at hand...

4 ^ v . Reply . Share

Thursday, January 11, 2018

The Tribune

VOICE OF THE PEOPLE

facebook

Google+

HOME | NATION | WORLD | PUNJAB | HARYANA | HIMACHAL | J & K | UTTARAKHAND | CITIES | OPINION | SPORT | BUSINESS | FEATURES

Nation

Posted at: Jan 4, 2018, 1:54 PM; last updated: Jan 4, 2018, 2:11 PM (IST)

UIDAI denies any breach of Aadhaar data

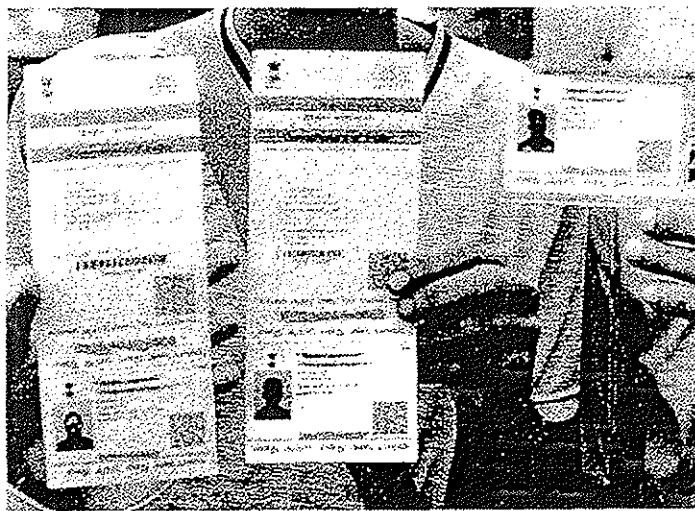


Photo for representational purpose only.

Tribune News Service
New Delhi, January 4

Responding to The Tribune exclusive story revealing how UIDAI data on Aadhaar number holders is being accessed by unauthorised agents, the Unique Identification Authority of India (UIDAI) today claimed it was a case of "misreporting", and that there had been no Aadhaar data breach.

The following is the statement issued by the UIDAI, reproduced verbatim:

"Unique Identification Authority of India (UIDAI) has denied the media report published in The Tribune titled **"Rs 500, 10 minutes, and you have access to billion Aadhaar details"** and has said that it is a case of misreporting. UIDAI assured that there has not been any Aadhaar data breach. The Aadhaar data including biometric information is fully safe and secure.

(Follow [The Tribune on Facebook](#); and [Twitter @thetribunechd](#))

In a statement issued today UIDAI said that UIDAI has given the said search facility for the purpose of grievance redressal to the designated personnel and state government officials to help residents only by entering their Aadhaar number/EID. UIDAI maintains complete log and traceability of the facility and any misuse can be traced and appropriate action taken. The reported case appears to be instance of misuse of the grievance redressal search facility. As UIDAI maintains complete log and traceability of the facility, the legal action including lodging of FIR against the persons involved in the instant case is being done.

UIDAI reiterates that the grievance redressal search facility gives only

Related Articles

Rs 500, 10 minutes, and you have access to billion Aadhaar details

Also in this section

BJP draws parallel between Siddaramaiah and Hafiz Saeed

Tibetan PM-in-exile cautions India against China

No point in securing Aadhaar data now: Chidambaram

US Ambassador bats for India-US Free Trade Agreement

In London, Rijiju seeks UK help in early extradition of Mallika

TOP STORIES



India, Pak NSAs met in Thailand, 'talks on terror' can go ahead: MEA



Justice Dhingra to supervise probe into 186 anti-Sikh riot cases



Supreme Court to hear pl for probe into CBI judge Loya's death



Nitin Gadkari's earful for naval top brass for 'obstructing development'



Indu Malhotra first woman lawyer to be directly appointed as SC judge

CITY FOCUS

Chandigarh



Woman, daughter put up brave fight

11 Jan 2018 | 1:55 AM

CHANDIGARH: Ritu Jain, a jewellery

designer, who, along with her daughter and a servant, was present in the house in Sector 22 when the robbery took place, was injured after she tried to fight the robbers.

Dog bite hurts more as dispensaries sans vaccine

PU Prof dies of cardiac arrest in Rajasthan

GMADA set to offer 900 residential plots

2 women among three held for minor rape, murder

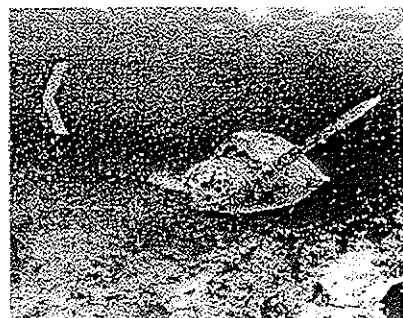
30-yr-old convicted of widow's rape

Ex-Mayor was controversy's child

Day of bouquets

more Chandig

SCI/TECH/GADGETS/ENV.



Warming turning major sea turtle population female

more Sci

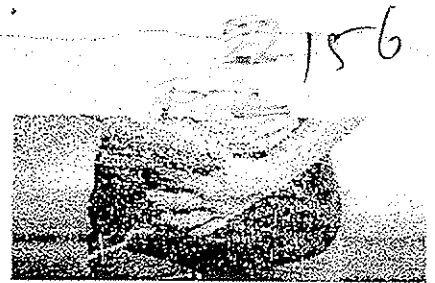
HEALTH



biometric database which remains fully safe and secure with highest encryption at UIDAI and mere display of demographic information cannot be used without biometrics.

Further, the Aadhaar number is not a secret number. It is to be shared with authorized agencies whenever an Aadhaar holder wishes to avail certain service or benefit of government welfare scheme/s or other services. But that does not mean that the proper use of Aadhaar number poses a security or financial threat. Also, mere availability of Aadhaar number will not be a security threat or will not lead to financial/other fraud, as for a successful authentication fingerprint or iris of individual is also required.

Claims of bypassing or duping the Aadhaar enrolment system are totally unfounded. Aadhaar data is fully safe and secure and has robust uncompromised security. The UIDAI Data Centres are infrastructure of critical importance and is protected accordingly with high technology conforming to the best standards of security and also by legal provisions."



New swallowable sensors to monitor human gut health

more Health

COMMENTS

All readers are invited to post comments responsibly. Any messages with foul language or inciting hatred will be deleted. Comments with all capital letters will also be deleted. Readers are encouraged to flag the comments they feel are inappropriate. The views expressed in the Comments section are of the individuals writing the post. The Tribune does not endorse or support the views in these posts in any manner.

7 Comments [tribuneindia](#)

Login

Recommend Share

Sort by Best



Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name



mu shankar · 7 days ago

UIDAI is joking.

1 ^ v · Reply · Share



Tukaram_2009 · 7 days ago

UIDAI and the govt of India are always in a denial mode about data leak

1 ^ v · Reply · Share



Harjinder Singh Sandhawalia · 7 days ago

India is full of scammers. They want to become rich right way. Remember the call centers cyber crimes they were cheating Americans on IRS tax issues. The Indian authorities are so dumb or part of the the scam.

^ v · Reply · Share



XANZY · 7 days ago

Disgusting adg and ed officers

^ v · Reply · Share



XANZY · 7 days ago

Aadhaar officials of chandigarh should be punished as they deny for any data leakage. specially Adg jindal officer. Its damn Aadhaar Scam

^ v · Reply · Share



Kest · 7 days ago

UIDAI is still insisting that their data is "safe and secure" even after the gigantic breach has been proven by the reporter. Maybe UIDAI is referring to the fact that their own servers have not been stolen. That is their limited definition of "data security".

^ v · Reply · Share



Neelkamal Chadhe · 4 days ago

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

157
Annexure R-3

WRIT PETITION (CIVIL) NO. 1056 OF 2017

Nachiket Udupa & Another ... PETITIONERS

VERSUS

Union of India & Others ... RESPONDENTS

AND

WRIT PETITION (CIVIL) NO. 833 OF 2013

Aruna Roy & Another ... PETITIONERS

VERSUS

Union of India & Others ... RESPONDENTS

WRITTEN SUBMISSIONS ON BEHALF OF
MR. K. V. VISWANATHAN
SR. ADVOCATE

I. INTRODUCTION.....	1
A. Petitions before this Hon'ble Court.....	1
B. Constitutional tests and breaches	1
C. All acts done prior to the passage of the Act are void <i>ab initio</i> , and are not saved/validated by Sec. 59. In any event, sec. 59 is invalid	2
 II. COLLECTION OF IDENTITY INFORMATION UNDER THE AADHAAR ACT [SEC. 3, 4(3), 7 & ALLIED SECTIONS AND REGULATIONS] VIOLATES ART. 14 AND ART. 21	4
A. The Aadhaar Act and surrounding infrastructure has made possession of Aadhaar <i>de facto</i> mandatory	4
B. Compulsory collection of identity information violates various facets of the right to privacy	5
(i) Bodily Privacy.....	5
(ii) Decisional Privacy.....	6
(iii) Informational Privacy.....	7
C. Compulsion by the State vis-à-vis non-State actors.....	7
D. State compulsion, by Aadhaar, is neither proportionate nor reasonable.....	7
(i) Limits of compulsion by law on individual freedoms.....	7
(a) Compulsion as punishment for law-breaking	8
(b) Compulsion as an aid to law-enforcement	8
(c) Compulsion to prevent law breaking	8
(ii) Limits of bodily integrity in medical jurisprudence	9
(iii) The presumption of criminality inherent in the collection of identity information under the Act is disproportionate and arbitrary	10
E. The Act is unconstitutional since it collects the identity information of children between 5-18 years without parental consent.....	11

III. CENTRALISED STORAGE OF PERSONAL DATA UNDER THE AADHAAR ACT [SEC. 2(C), 2(H), 8(4), 10, 28(5), 32, 37, & ALLIED SECTIONS AND REGULATIONS] IS DISPROPORTIONATE AND VIOLATES ART. 14 & 21 12

- A. Centralised storage of identity information is disproportionate..... 12
- B. Unduly long retention period of transaction data and authentication records is disproportionate..... 12
- C. The Act and Regulations preclude Aadhaar number holders from accessing or correcting their identity information stored on the CIDR 13
- D. The Act & Regulations lack safeguards to secure sensitive personal data 14

IV. USE OF IDENTITY INFORMATION UNDER THE AADHAAR ACT [SEC. 3(2), 7, 8, 29, 31(2), 33, 57 & ALLIED SECTIONS AND REGULATIONS] IS DISPROPORTIONATE, ARBITRARY, AND EXCLUSIONARY..... 15

- A. The legal framework of the Aadhaar Act that governs the use of information fails to meet constitutional standards 15
 - (i) *The Act lacks any purpose limitation*..... 15
 - (ii) *The Regulations governing the use of the stored identity information are vague.* 16
 - (iii) *Section 33 of the Act governing the disclosure of information in certain cases is disproportionate, contrary to principles of natural justice, and unconstitutional* 16
 - (iv) *The use of the Aadhaar infrastructure by private entities is unconstitutional* 17
- B. Section 7 of the Aadhaar Act is unconstitutional and violates Art. 14 18
 - (i) *Factual foundation: Systematic exclusion caused by Aadhaar*..... 18
 - (ii) *Design and operation of the Aadhaar program is inherently arbitrary* 19
 - (a) Reliance on a probabilistic system of biometric authentication is arbitrary .. 19
 - (b) Violation of rights cannot be left to vagaries of administrative discretion 20
- C. Section 7 of the Aadhaar Act is unconstitutional and violates Art. 21 20
 - (i) *Mandatory authentication at the point of use violates Article 21*..... 20
 - (ii) *The government has failed to discharge its burden of proof under Art. 21* 21
 - (a) Proportionality, burden of proof, standards of review 22
 - (b) Failure to demonstrate that Aadhaar has caused significant savings – illustrated in the PDS Scheme..... 23
 - (c) Failure to consider less-invasive & effective alternate identification methods 25

WRITTEN SUBMISSIONS – II
ON BEHALF OF K. V. VISWANATHAN
SENIOR ADVOCATE

- V. THE AADHAAR ACT [SEC. 2(g), 2(j), 2(k) & 23(2)] SUFFERS FROM EXCESSIVE DELEGATION AND THE ALLIED REGULATIONS ARE VAGUE, MANIFESTLY ARBITRARY, AND UNREASONABLE.....1
- VI. NO RIGHT OF HEARING AGAINST OMISSION & DEACTIVATION OF AADHAAR NUMBERS, VIOLATING PRINCIPLES OF NATURAL JUSTICE.....2
- VII. THE MOBILE LINKING DIRECTION DATED 23.03.2017 IS ULTRA VIRES.....4

regulating its use, also renders the Aadhaar scheme violative of Art. 21. These records are metadata inasmuch as they provide a detailed picture of an Aadhaar number holder's activities, and give excessive power to the State and private entities.

47. Indeed, the long-term storage of transaction records is contrary to the core purpose of Aadhaar, which is to eliminate identity theft by correctly identifying a beneficiary through biometric authentication. The purpose of Aadhaar, therefore, is fulfilled *at the time of* authentication. Any further, or prolonged, storage, is disproportionate, and fails the Art. 14 test of arbitrariness. Notably, the retention of such sensitive data for long periods of time was held to be disproportionate by the ECJ (GC) in *Digital Rights Ireland Ltd v Minister for Communications*, C-293/12 (2014), ¶¶51-60, 62, 66 @pg 118-20, Vol. IV, especially since access to retained data was not dependant on a prior judicial/administrative review.

[See also:

- (i) *MK v France*, (2013) ECHR 341, ¶¶ 29, 32-43 @pg 185-188, Vol. IV
- (ii) *Peruzzo & Martens v Germany*, (2013) ECHR 743, ¶ 44-47 @pg 204-205, Vol. IV
- (iii) *S & Marper*, ¶¶ 86, 103-107, 112, 119-121 @pg 228, 234-237, Vol. II²¹
- (iv) *R v Commr of Police*, [2011] UKSC 21, ¶¶ 1, 27 @pg 124, 132, Vol. IV]

C. THE ACT AND REGULATIONS PRECLUDE AADHAAR NUMBER HOLDERS FROM ACCESSING OR CORRECTING THEIR IDENTITY INFORMATION STORED ON THE CIDR

48. The citizen's right to know, derived from Arts. 19(1)(a) and 21, includes the right to receive information,²² and hence, access and control one's own personal data. The globally accepted privacy principles, as recognised by the **Report of the Group of Experts (2012)** @pg 7, 17 Vol. IV, include such a right to "access and correction", which confers in every individual a *right* to (a) access their personal data; (b) correct, amend or delete inaccurate information; and (c) know the nature of personal information stored by data controller.
49. However, the Aadhaar Act and accompanying Regulations deprive Aadhaar number holders of the right to access and correct their personal information. At the outset, the proviso to **sec. 28(5)** of the Act denies individuals the right to access *their own* core biometric information stored in the CIDR. This amounts to an impermissible waiver of rights under Arts. 19(1)(a) and 21 since it divests Aadhaar number holders from any modicum of control over their information [See *Baseshshar Nath v CIT*, AIR 1959 SC 149, ¶ 12-15 @pg 260, 263 Vol. IV and *Puttaswamy*, ¶ 126].
50. Despite recognising some right to access information under **sec. 3(2)(c)** and authentication records under **sec. 32(2)**, the Act and Regulations do not provide any measure by which such rights can be enforced:

²¹ *Marper* held that permanent retention of fingerprints, without possibility of deletion, when they were being regularly processed by automated means for criminal-identification purposes is disproportionate.

²² See *Indian Soaps & Toiletries Makers Association*, (2013) 3 SCC 641, ¶28 and 29 @pg 221, Vol. IV and *Reliance Petrochemicals v Indian Express*, (1988) 4 SCC 592 ¶34 @pg 246, Vol. IV.

- (a) **Regulation 9(c) of Enrolment Regulations** states that the Aadhaar number holder has a “right to access information”, with the procedure for making such requests for access provided in Schedule I. However, **Schedule I** only states, “*I have a right to access my identity information (except core biometrics) following the procedure laid down by UIDAI*”. Thus, despite cross-citing each other, no procedure is laid down.
- (b) **Regulation 3(3) of Sharing of Information Regulations** states that the UIDAI “shall” share authentication records of the Aadhaar number holder with them in accordance with **Regulation 28 of Authentication Regulations**; which in turn states that the right to access authentication records is “subject to conditions” prescribed by the UIDAI. Further, **Regulation 28(1)** grants the right to access one’s authentication records “*within the period of retention of such records before they are archived*”, which as per **Regulation 27(1)** is only 6 months. Thus, even though an individual’s authentication transaction data is “archived” by the UIDAI for five years (after the expiry of the 6 month period), she is only entitled to access it during the 6 months.
- (c) **Regulation 4(3) of Sharing Regulations** states that private requesting entities “may” share the authentication logs of an Aadhaar number holder with them upon their request, with no recourse to the Aadhaar number holder if such a request is denied.

51. Consequently, the absence of a right to access one’s core biometric data, the lack of guidelines, independent review or appeal represents a failure of the State to fulfil its positive obligations of providing unimpeded access (and hence, correction) to residents’ of their own data [See *MG v UK*, (2003) 36 EHRR 3, ¶¶27, 31]

D. THE ACT & REGULATIONS LACK SAFEGUARDS TO SECURE SENSITIVE PERSONAL DATA

52. This Hon’ble Court in *Puttaswamy* [per Kaul J., ¶ 638] and earlier in *A.K Roy*, (1982) 1 SCC 271, ¶ 35 @pg 340, Vol. IV made it clear that for any law to be constitutionally valid, it must contain certain minimum procedural guarantees, to ensure due process and reasonableness under Art. 21.²³ However, the Act and Regulations do not contain such minimum guarantees, and thus, fail the test under Art. 21 of the Constitution.

53. First, no “information security policy”, as required under **Regulation 3, Data Security Regulations**, has been specified by the UIDAI till date. Thus, the storage and regulation of access/use of vast swathes of collected personal data is being done in a legal vacuum. Around 210 websites of Central & State Government departments and some educational institutes have publicly displayed names, address, and Aadhaar numbers of beneficiaries. However, no punitive action was taken against the concerned officials, except for issuing general directions to the departments to remove the Aadhaar data from their websites. [See

²³ See *Dr N.B. Khure v State of Delhi*, [1950] SCR 519 @pg386, Vol. IV and *PUCI v UOI*, (1997) 1 SCC 301, @pg 412, Vol. IV in the Indian context. See *S & Marper*, (supra), ¶ 99, 103 @ pg 232-33, Vol. II; *X v Finland*, (supra) ¶ 220-21 @pg 559, Vol. III; *Peruzzo & Martens* (supra), ¶ 47 @pg 205, Vol. III; and *Z v. Finland*, (1997) ECHR 10, ¶ 95, 112, 114 @pg 439, 444-45, Vol. IV for ECHR.

Reply dated 03.01.2018 to Unstarred Qs No. 2582 in the Lok Sabha @pg 18A, Vol. IV]. Notably, sec. 37 only criminalises *intentional* disclosure or dissemination of identity information, and not negligent instances of breach, further evidencing lack of safeguards.

54. It is now well-recognised that centralised biometric databases are not secure, and the Aadhaar infrastructure, in particular is susceptible to data breaches, especially due to its use of biometrics as authentication credentials. Such concerns also led to scrapping of a similar project in the UK.²⁴
 55. Unlike a credit card or financial transaction, breach of biometric information cannot be reversed. More egregiously, the Aadhaar Act does not include a data breach notification principle, as recommended by the **Report of the Group of Experts (2012) @pg 16, Vol. IV**, to inform the Aadhaar number holder of any breach of personal data.
 56. Further, **Regulation 4(2)(b) of the Authentication Regulation** recognises the OTP-based mode of authentication, which is also used under the e-KYC authentication facility u/**Regulation 3(ii)**. OTP authentication is often used when biometric authentication fails. However, OTP authentication defeats the objective of preventing identity fraud, since all it requires is a phone number and/or email address, which, as per **Regulation 4(2)(i) read with 10(5) read with Schedule III of the Aadhaar Enrolment Regulations** need not be registered and verified at the time of getting an Aadhaar.
- IV. **USE OF IDENTITY INFORMATION UNDER THE AADHAAR ACT [SEC. 3(2), 7, 8, 29, 31(2), 33, 57 & ALLIED SECTIONS AND REGULATIONS] IS DISPROPORTIONATE, ARBITRARY, AND EXCLUSIONARY**
57. Fundamental rights are violated at the point of use of identity information under the Act in two ways. *First*, the legal framework to govern the manner in which personal data might be used lacks purpose limitation, limited disclosure and permits use by private entities. *Second*, the mandate of sec. 7 of the Act to use Aadhaar as a compulsory form of identification and authentication for availing entitlements violates Art. 14 & 21, since by design, it is exclusionary, arbitrary and disproportionate.
 - A. **THE LEGAL FRAMEWORK OF THE AADHAAR ACT THAT GOVERNS THE USE OF INFORMATION FAILS TO MEET CONSTITUTIONAL STANDARDS**
 - (i) *The Act lacks any purpose limitation*
 58. Two key inter-related principles of privacy relate to collection and purpose limitation, which require a data controller to *collect* only such data as is necessary for the identified purpose; and to then process and *use* such collected data only for the stated purpose and

²⁴ In the UK context, the **Report of LSE, The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications**, 2005, pg110 @p. 67, Vol. IV cautioned against the centralisation of a biometric database with valuable citizen information, highlighted the untested and unreliable nature of such technology, the high risk of failure, increased security threats, and the unacceptable imposition on citizens, which led to the Bill being scrapped.

162
Annexure R-4

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. 1056 OF 2017

Nachiket Udupa & Another

... PETITIONERS

VERSUS

Union of India & Others

... RESPONDENTS

ALONG WITH W.P. (C) No. 833/2013

COMPILATION ON BEHALF OF MR. K.V. VISWANATHAN, SR. ADVVOLUME - IV
CENTRALISED DATA STORAGE, BREACH & ACCESS

S.NO.	PARTICULARS	PAGE NO
A. DATA BREACH & BEST PRACTICES		
1.	Report of the Group of Experts on Privacy constituted by Planning Commission (Oct. 16, 2012) [RELEVANT EXTRACTS]	1-18
2.	Reply to Unstarred Question [No. 2582] on "Breach of Aadhaar Data" in the Lok Sabha (Jan. 03, 2018)	18A
3.	<i>Rs. 500, 10 minutes, and you have access to a billion Aadhaar details</i> , THE TRIBUNE (Jan. 04, 2018)	19-21
4.	UIDAI Press Note (Jan. 04, 2018)	22
5.	Shweta Agrawal <i>et al</i> , <i>Privacy and Security of Aadhaar: A Computer Science Perspective</i> , 52(37) ECON. & POL. WEEKLY (16 Sept. 2017)	23-37
6.	Relevant extracts from 'LSE, <i>The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications</i> ' (Jun. 2005)	38-68
B. RIGHT AGAINST DATA AGGREGATION		
7.	Leander v. Sweden (1987) ECHR 4, ¶ 48	RefVOL II
8.	Amann v. Switzerland (2000) ECHR 88 (Grand Chamber), ¶ 69	RefVOL II
C. RIGHT AGAINST PROLONGED DATA RETENSION		
9.	Digital Rights Ireland Ltd v. Minister for Communications [2015] QB 127 [ECJ], ¶33, 44-66	69-121 @pg 102 onwards
10.	S & Marper v. UK	RefVOL II

	(2008) ECHR 1581, ¶ 86, 104-107, 112, 119-121	
11.	R v. Commissioner of Police [2011] UKSC 21, ¶¶ 1, 26 & 27	122-174
12.	MK v. France (2013) ECHR 341, ¶¶ 29, 32-43	175-189
13.	Peruzzo & Martens v. Germany (2013) ECHR 743 ¶¶ 33, 44-47	190-207
D. RIGHT TO ACCESS INFORMATION & PERSONAL DATA		
14.	Indian Soaps & Toiletries Makers Association (2013) 3 SCC 641, ¶¶ 28 & 29	208-224
15.	Reliance Petrochemicals v. Indian Express (1988) 4 SCC 592, ¶ 34	225-251
E. NO WAIVER OF FUNDAMENTAL RIGHTS		
16.	Baseshshar Nath v CIT AIR 1959 SC 149 (<i>Das C.J.</i>), ¶ 14-15	252-309
F. RIGHT TO PROCEDURAL SAFEGAURDS		
17.	Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (<i>Kaul J.</i>), ¶ 638	Ref. SCC
18.	A.K Roy v. Union of India (1982) 1 SCC 271, ¶ 35	310-380
19.	Dr. N. B. Khare v. State of Delhi [1950] SCR 519	381-398
20.	Peoples' Union for Civil Liberties v. Union of India (1997) 1 SCC 301, ¶ 34	399-416
21.	S & Marper v. UK (2008) ECHR 1581, ¶ 99	Ref VOL. II
22.	X v Finland (2012) ECHR 1371, ¶¶ 220 & 221	Ref. VOL. III
23.	Peruzzo & Martens v Germany 7841/08 & 57900/12 ECHR (Jun. 04, 2013) ¶ 47	<i>Supra</i>
24.	Z v. Finland (1997) ECHR 10 ¶¶ 95 & 112-114	417-451

163

164
B.F.

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2582
TO BE ANSWERED ON 03-01-2018

BREACH OF AADHAAR DATA

2582. **SHRI AJAY MISRA TENI:**
SHRI J.C. DIVAKAR REDDY:
SHRIMATI KOTHAPALLI GEETHA:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that names and addresses of some Aadhaar cardholders were made public on more than 200 websites of Central and State Governments as per Unique Identification Authority of India (UIDAI);

(b) if so, the details thereof;

(c) the action taken by the Government against the departments of Central and State Government and education institutes and private organisations who have made the names and address of Aadhaar cardholders public;

(d) whether any steps have been taken by the Government to ensure that the information of Aadhaar cardholders is not made public by any Government and private department; and

(e) if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION
TECHNOLOGY
(SHRI ALPHONS KANNANTHANAM)

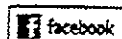
(a) and (b): Yes, Sir. It was found that approximately 210 websites of Central Government, State Government departments and some educational institutes were displaying the list of beneficiaries along with their name, address, other details and Aadhaar numbers for information of general public.

(c) to (e): The concerned departments/websites were instructed to remove the Aadhaar and other personal data from the said websites. In addition, the Central and State Governments have been advised to sensitize all Ministries/ Departments to take all precautions while publishing or sharing data on their websites and ensure compliance of Aadhaar Act, 2016 and Information Technology Act, 2000.

Wednesday, February 21, 2018

The Tribune

VOICE OF THE PEOPLE



Follow @tribuneindia

Google+

HOME | NATION | WORLD | PUNJAB | HARYANA | HIMACHAL | J & K | UTTARAKHAND | CITIES | OPINION | SPORT | BUSINESS | FEATURES

Nation

Posted at: Jan 4, 2018, 2:07 AM; last updated: Jan 5, 2018, 1:58 PM (IST)

TRIBUNE INVESTIGATION — SECURITY BREACH

Rs 500, 10 minutes, and you have access to billion Aadhaar details

Group tapping UIDAI data may have sold access to 1 lakh service providers



Rachna Khaira
Tribune News Service
Jalandhar, January 3

It was only last November that the UIDAI asserted that "Aadhaar data is fully safe and secure and there has been no data leak or breach at UIDAI." Today, The Tribune "purchased" a service being offered by anonymous sellers over WhatsApp that provided unrestricted access to details for any of the more than 1 billion Aadhaar numbers created in India thus far.

(Follow [The Tribune on Facebook](#); and [Twitter @thetribunechd](#))

It took just Rs 500, paid through Paytm, and 10 minutes in which an "agent" of the group running the racket created a "gateway" for this correspondent and gave a login ID and password. Lo and behold, you could enter any Aadhaar number in the portal, and instantly get all particulars that an individual may have submitted to the UIDAI (Unique Identification Authority of India), including name, address, postal code (PIN), photo,

Related Articles

UIDAI denies any breach of Aadhaar data

Aadhaar data breach finds mention in Parliament

Aadhaar data breach shocks Twitterati, top trend for the day

Also in this section

Rotomac: Kothari, son in CBI custody

Kanpur tycoon: Stationery czar to loan defaulter

PNB scam: SC to hear plea seeking SIT probe today

Naxal-hit Malkangiri to get first rail line

Two Sangma dynasties vie to rule Meghalaya

TOP STORIES



Delhi Chief Secretary accuses AAP MLAs of assault in CM's presence



AAP's counter: Leaders attacked, Delhi CS made casteist remarks



Margins on drugs as high as 1,192% in 4 pvt hospitals: Pricing regulator



3 dead, 11 injured after ammonia gas leak near Rajpura in Patiala



First big arrest in PNB fraud: Vipul Ambani held by CBI

CITY FOCUS

Chandigarh



Mohali MC to take up tax waiver to QuarkCity

21 Feb 2018 | 1:57 AM

MOHALI: The Punjab

Government and the Mohali

Municipal Corporation are likely to come face to face on the issue of waiving property tax of the QuarkCity India Private Limited project at the Phase 8 Industrial Area here.

Missing child found dead in water tank at home

HC seeks status report on illegal construction in Sukhna vicinity

Old boy gifts Rs 1 crore to St John's

Dadu Majra stink reaches PMO

Docs to examine Bheora's mother

UIDAI goof-up: Twin Aadhaar for toddler

Five anganwadis at Kumbra village sans ration for months

more Chandigarh...

SCI/TECH/GADGETS/ENV.



name, address, phone number and email.

What is more, The Tribune team paid another Rs 300, for which the agent provided "software" that could facilitate the printing of the Aadhaar card after entering the Aadhaar number of any individual.

When contacted, UIDAI officials in Chandigarh expressed shock over the full data being accessed, and admitted it seemed to be a major national security breach. They immediately took up the matter with the UIDAI technical consultants in Bangalore.

Sanjay Jindal, Additional Director-General, UIDAI Regional Centre, Chandigarh, accepting that this was a lapse, told The Tribune: "Except the Director-General and I, no third person in Punjab should have a login access to our official portal. Anyone else having access is illegal, and is a major national security breach."

1 lakh illegal users

Investigations by The Tribune reveal that the racket may have started around six months ago, when some anonymous groups were created on WhatsApp. These groups targeted over 3 lakh village-level enterprise (VLE) operators hired by the Ministry of Electronics and Information Technology (ME&IT) under the Common Service Centres Scheme (CSCS) across India, offering them access to UIDAI data.

CSCS operators, who were initially entrusted with the task of making Aadhaar cards across India, were rendered idle after the job was withdrawn from them. The service was restricted to post offices and designated banks to avoid any security breach in November last year.

Spotting an opportunity to make a quick buck, more than one lakh VLEs are now suspected to have gained this illegal access to UIDAI data to provide "Aadhaar services" to common people for a charge, including the printing of Aadhaar cards. However, in wrong hands, this access could provide an opportunity for gross misuse of the data.

The hackers seemed to have gained access to the website of the Government of Rajasthan, as the "software" provided access to "aadhaar.rajasthan.gov.in", through which one could access and print Aadhaar cards of any Indian citizen. However, it could not be ascertained whether the "portals" were genuinely of Rajasthan, or it was mentioned just to mislead.

Sanjay Jindal said all of this could be confirmed only after a technical investigation was conducted by the UIDAI.

'Privacy at risk'

"Leakage of Aadhaar data reveals that the project has failed the privacy test. At the recently concluded 11th WTO Ministerial Conference, India submitted a written position on e-commerce, opposing the demand for negotiations on e-commerce by the US and its allies. The latter were demanding access to citizens' database for free. The revelation by The

Back-and-forth exchanges boost children's brain response to language

more Sci/Tech...

HEALTH



Eating yogurt may reduce risk of heart diseases

more Health...

167

Tribune also means that the proposed data protection law will now hold no purpose, as the data has already been breached. The state governments must immediately disassociate themselves and cancel the MoU signed with UIDAI," said Gopal Krishan, New Delhi-based convener of the Citizens Forum for Civil Liberties, who appeared before the Special Parliamentary Committee that examined the Aadhaar Bill in 2010.

A quick chat, and full access

- 12:30 pm: This correspondent posing as 'Anamika' contacted a person on WhatsApp number 7610063464, who introduced himself as 'Anil Kumar'. He was asked to create an access portal.
- 12:32pm: Kumar asked for a name, email ID and mobile number, and also asked for Rs 500 to be credited in his Paytm No. 7610063464.
- 12:35 pm: This correspondent created an email ID, aadharjalandhar@gmail.com, and sent mobile number *****5852 to the anonymous agent.
- 12:48 pm: Rs 500 transferred through Paytm.
- 12:49 pm: This correspondent received an email saying, "You have been enrolled as Enrolment Agency Administrator for 'CSC SPV'. Your Enrolment Agency Administrator ID is 'Anamika_6677'." Also, it was said that a password would be sent in a separate mail, which followed shortly.
- 12:50 pm: This correspondent had access to the Aadhaar details of every Indian citizen registered with the UIDAI.

Printing Aadhaar card

This correspondent later again approached Anil Kumar to ask for software to print Aadhaar cards. He asked for Rs 300 through Paytm No. 8107888008 (in the name of 'Raj'). Once paid, a person identifying himself as Sunil Kumar called from mobile number 7976243548, and installed software on this correspondent's computer by accessing it remotely through "TeamViewer". Once the job was done, he deleted the software drivers, even from the recycle bin.

Possible misuse

Getting SIM cards, or bank accounts in anyone's name. Last month, a man was arrested in Jalandhar for withdrawing money from someone's bank account by submitting a fake Aadhaar card.



Sitaram Yechury
@SitaramYechury

The perils of making Aadhaar mandatory and linking it to bank accounts, as insisted upon by Modi govt, are visible here. Do we need more proof to stop this madness?

tribuneindia.com/news/nation/rs...

9:06 AM - Jan 4, 2018

Rs 500, 10 minutes, and you have access to ...

JALANDHAR: It was only last November that the UIDAI asserted that "Aadhaar data is fully safe and secure and there has been no data leak or

tribuneindia.com

168

Unique Identification Authority of India (UIDAI)
Press Note
4.01.2018

New Delhi. Unique Identification Authority of India (UIDAI) has denied the media report published in The Tribune titled "Rs 500, 10 minutes, and you have access to billion Aadhaar details" and has said that it is a case of misreporting. UIDAI assured that there has not been any Aadhaar data breach. The Aadhaar data including biometric information is fully safe and secure.

In a statement issued today UIDAI said that UIDAI has given the said search facility for the purpose of grievance redressal to the designated personnel and state government officials to help residents only by entering their Aadhaar number/EID. UIDAI maintains complete log and traceability of the facility and any misuse can be traced and appropriate action taken. The reported case appears to be instance of misuse of the grievance redressal search facility. As UIDAI maintains complete log and traceability of the facility, the legal action including lodging of FIR against the persons involved in the instant case is being done.

UIDAI reiterates that the grievance redressal search facility gives only limited access to name and other details and has no access to biometric details. UIDAI reassures that there has not been any data breach of biometric database which remains fully safe and secure with highest encryption at UIDAI and mere display of demographic information cannot be misused without biometrics. Further, the Aadhaar number is not a secret number. It is to be shared with authorized agencies whenever an Aadhaar holder wishes to avail certain service or benefit of government welfare scheme/s or other services. But that does not mean that the proper use of Aadhaar number poses a security or financial threat. Also, mere availability of Aadhaar number will not be a security threat or will not lead to financial/other fraud, as for a successful authentication fingerprint or iris of individual is also required.

Claims of bypassing or duping the Aadhaar enrolment system are totally unfounded. Aadhaar data is fully safe and secure and has robust uncompromised security. The UIDAI Data Centres are infrastructure of critical importance and is protected accordingly with high technology conforming to the best standards of security and also by legal provisions.

#####

Privacy and Security of Aadhaar: A Computer Science Perspective

Shweta Agrawal Subhashis Banerjee Subodh Sharma
Computer Science and Engineering, IIT Delhi
New Delhi 110016

Abstract—We investigate the privacy and security issues of Aadhaar from a technology point of view. Specifically, we investigate the possibilities of identification and authentication without consent using the Aadhaar number or biometric data, and unlawful access of Aadhaar data in the central repository. Our analysis suggests that privacy protection in Aadhaar will require a) an independent third party that can play the role of an online auditor, b) study of several modern tools and techniques from computer science, and c) strong legal and policy frameworks that can address the specifics of authentication and identification in a modern digital setting.

Index Terms—Computer Science, privacy, security, cryptography, authentication, identification

I. INTRODUCTION

The Aadhaar project is the world's largest national identity project, launched by government of India, which seeks to collect biometric and demographic data of residents and store these in a centralised database. To date, 1036 million users have enrolled in the system, and the government has spent at least 890 million USD on the project (Wikipedia, 2016a). However, recently there has been considerable deliberations over the privacy and security issues related to the Aadhaar project. In this article, we examine these issues from a Computer Science perspective.

A. Background

Privacy concerns relating to the Aadhaar project have been the subject of much heated debate recently (Express News Service, 2016; NDTV, 2016a). On the one hand, positions taken by the government and UIDAI on these issues have been ambiguous. Arguing before a bench in the Supreme Court, the Attorney General of India has claimed that Indian citizens have no constitutional right to privacy (PTI, 2015). This is surprising not only because there are several interpretations of constitutional provisions and judgements to the contrary (Bhatia, 2015; Kumar, 2015), but also because it contravenes conventional wisdom and best practices in digital authentication

and authorisation systems (Diffie & Hellman, 1979; Wikipedia, 2016l.g). The finance minister, while getting the Aadhaar bill passed as a money bill, announced that "the government presupposes privacy as a fundamental right" and claimed that the bill has tightened privacy provisions when compared to what was there in the previous version (Scroll Staff, 2016). However, neither the government nor the UIDAI makes it clear what precisely are the privacy concerns that are being addressed, what precisely are the methods being deployed and why the resulting proposal is secure. The UIDAI does describe the security measures it has put in place (UIDAI, 2014), but does not provide an analysis of the measures with respect to perceived threat levels and potential privacy breaches. This has resulted in an overall confusion about the impact on privacy engendered by the Aadhaar project.

On the other hand, several civil society activists and social commentators (Arun, 2016; Mehta, 2016; Jayaram, 2015; Vombarkere, 2016; Makkar, 2016; Duggal, 2011; Dréze, 2016) have expressed concerns about the weak privacy provisions in the Aadhaar project and bill. However, while alerting to the possibilities of opening doors to mass surveillance, we feel that some of the commentaries have been unbounded in their criticisms and not entirely specific in their statements of concerns. The gist of most criticisms has been that it is necessarily unsafe to use biometrics and a unique identification number, and to store biometric and demographic data as well as authentication trails in a central repository. However, whether breach of privacy is inevitable, and whether there may exist technological and legal provisions which can make Aadhaar safe are important questions that have not been adequately addressed. We note that some crucial lacunae in the identification and authentication processes of Aadhaar have been pointed out in (Centre for Internet & Society, 2016), which also makes several important suggestions including implementation of recommendations of Shah (The Planning Commission: Government of India, 2011) and Sinha (Lok Sabha Secretariat: New Delhi, 2012) committees.

170

Despite these, thorough analyses of the possible ways in which privacy can be breached, and possible counter-measures both from technological and legal perspectives, remain missing. In this note we endeavour to fill in some of this gap from a technology point of view.

B. Perspectives on Aadhaar: pros and cons

At its core, the Aadhaar act attempts to create a method for identification of individuals so as to provide services, subsidies and other benefits to the residents of the country. While the effectiveness of Aadhaar to the extent claimed in preventing leakages in social welfare schemes has been questioned (Khera, 2011, 2015; Zhong, 2016), the advantages of computerisation and reliably maintaining eligibility and distribution records in digital forms are well accepted (Masiero, 2015; Khera, 2013). Any digitisation requires indexes or unique ids, and in social welfare schemes local unique ids like ration or job card numbers are typically used. Standardising the digital record keeping processes across geographies and verticals, and linking the local ids with the unique national identities provided by Aadhaar, tantamount to virtually collating the different digital record tables into one. Though the digital records may still be geographically distributed, real-time access to the data, using the Aadhaar ids as handles, can then be provided to authorised central and state agencies for audit, monitoring, analysis and planning purposes. Thus, the Aadhaar number provides a single index across all services that may use Aadhaar.

Additionally, the Aadhaar project may provide the necessary impetus to standardisation and digitisation of other domains as well, many of which are long overdue. The Aadhaar ids can be used to create local ids for digitisation of new verticals easily. Even more importantly, Aadhaar can facilitate linking of local ids in currently isolated verticals like census, education, health-care and immunisation records, birth and death records, land records, property registration, income tax, banking, loans and defaults, police verification and law enforcement, disaster management, security and intelligence and such others. Thus, Aadhaar may not only enable efficient design, delivery, monitoring and evaluation of services in each domain individually, but also offers the possibility using modern data analytics techniques for finding large scale correlations in user data that may facilitate improved design of social policy strategies and early detection and warning systems for anomalies. For example, it may be tremendously insightful to be able to correlate education levels, family incomes and nutrition across the entire population; or disease spread

with income and education. More generally, it may enable carrying out econometric analysis, epidemiological studies, automatic discovery of latent topics and causal relationships across multiple domains of the economy (UN Global Pulse, 2012, 2016; Jennifer McNabb & Puckett, 2009; Krishnamurthy & Desouza, 2014; Varian, 2014; Einav & Levin, 2014, 2013; Athey & Imbens, 2015; Kleinberg *et al.*, 2015; McBride & Nichols, 2015). Indeed, extending the scope of Aadhaar from just being an identification and authentication system for social welfare schemes to a system which generates large scale data and facilitates automated analysis and planning, can potentially lead to far reaching benefits.

At the same time, apart from the concerns of loss of privacy and civil liberties, the Aadhaar project has attracted considerable criticism for causing significant disruptions and exclusions in social welfare schemes (Johari, 2016; NDTV, 2016b,a; Dréze, 2016; Yadav, 2016a,b), both due to careless deployment and uncertainties in biometric matching.

We believe that all the above issues, both for and against, require careful analysis and rigorous evaluation; and that the technological, legal and policy frameworks need to be considerably strengthened through debates and informed choices to evolve an effective national identity scheme.

C. Privacy and security concerns

We examine the following main concerns pertaining to privacy and security in Aadhaar:

- 1) Identification of individuals without consent using the global Aadhaar number.
- 2) Identification and authentication without consent using demographic and biometric data.
- 3) Surveillance, tracking or profiling of people beyond legal sanctions using the centralised database, either through external hacks or through insider leaks and collusion.

Specifically, we ask the following questions which we believe are crucial for ensuring safety of Aadhaar:

- 1) Is it possible to ensure that user data and identification and authentication trails are completely protected from manual inspection by the UIDAI or the Government or any other entity or individual, thereby effectively preventing unauthorised surveillance?
- 2) Is it possible to ensure that all transactions, investigations and analytics can be carried out in a safe way only through audited, pre-approved and tamper proof computer programs? Additionally, can it be ensured that the programs are true to

legal and policy frameworks, do precisely and only what they are supposed to do, and maintain tamper proof logs of all authorisation chains and results?

We believe that the above questions capture the essence of privacy protection in computerised databases. Privacy protection does not demand that data should not be collected, stored or used, but that there should be provable guarantees that the data cannot be used for any purpose other than those that have been approved.

D. Our Goal

Recent advances in Computer Science offer several novel and powerful solution ideas to address many of the privacy and security challenges posed by the project. Our goal is to carefully examine the security concerns, survey the technological tools that may aid us and provide a first order analysis of what might be feasible.

Our approach is as follows. We first capture the functionality desired by the Aadhaar project. Next, we analyse the security risks and vulnerabilities engendered by each entity and each communication link in the Aadhaar model. We examine the security measures proposed by UIDAI and discuss where these may be lacking. We elucidate recent tools from computer science, particularly from the fields of cryptography and security, which may assist in providing safeguards; this puts some stated concerns to rest while simultaneously raising multiple unforeseen issues. We summarise our key findings and recommendations in Table I in the concluding section (Section VII).

Overall, we hope that our work provides a rigorous and scientific treatment of privacy concerns regarding Aadhaar, and enables well informed and well reasoned decisions regarding deployment.

The rest of the paper is organised as follows. In Section II we describe the Aadhaar functional architecture, and the various entities involved and their roles; in Section III we analyse the privacy and security requirements of the Aadhaar project. In Section IV we discuss the subtle differences between identity verification and authentication and point out that failure to demarcate the two may lead to authentication without consent. In Section V we analyse the possibilities of privacy breaches through the Aadhaar number and suggest possible remedies. In Section VI we analyse the threats for potential privacy breaches from the Aadhaar database and the field devices and explore possible approaches that may be adopted to mitigate the risks. Finally, in Section VII we conclude the paper.

II. THE AADHAAR MODEL

In this section we describe the various entities involved in Aadhaar and their inter-dependencies, which will enable us to reason about its privacy and security requirements. The Aadhaar authentication and identity verification system comprises the following entities (UIDAI, 2016b):

- 1) The *Unique Identification Authority of India* (UIDAI) is responsible for providing the basic identification and authentication services. It provides a unique identifier (Aadhaar number) to each resident and maintains their biometric and demographic data in a *Central Identities Data Repository* (CIDR). The UIDAI manages the CIDR and provides identification and authentication services with yes/no answers.
- 2) An *Authentication User Agency* (AUA) who provides services to users that are successfully authenticated. Thus, an AUA connects to the CIDR and uses Aadhaar authentication to validate a user and enable its services. Examples of AUAs and services are banks, various state and central government ministries providing services such as the Public Distribution System (PDS), the National Rural Employment Guarantee Scheme (NREGS), and even private agencies like mobile phone operators. The responsibility of logistics of service delivery rests with the AUAs. In this federated model an AUA may choose to use only Aadhaar identification, or also authentication in conjunction with their own legacy identification and authentication systems. An AUA is required to enter in to a formal contract with UIDAI to be able to use Aadhaar authentication services.
- 3) An *Authentication Service Agency* (ASA) is an entity that has a secure leased line connectivity with the CIDR. ASAs transmit authentication requests to CIDR on behalf of one or more AUAs. An ASA enters into a formal contract with UIDAI.
- 4) The *users*, namely, the residents of the country who enrol themselves with UIDAI and are issued unique identification numbers (Aadhaar numbers). A user has to present this number as the basic identification to an AUA for availing Aadhaar authentication services. The Aadhaar number for a user is common across all AUAs and service domains.
- 5) The *Point of Sale* (POS) device, also known as authentication device which collects personal identity data from Aadhaar holders, prepares the information for transmission, transmits the authentication

172

tification packets for authentication and receives the authentication results.

- 6) An *Enrolment Station*, which is a collection of field devices used by enrolment agencies appointed by UIDAI to enrol people in to the Aadhaar database and capture their demographic and biometric particulars.

The Aadhaar number is common across all AUAs and service domains. The framework (without the enrolment station) is captured in Figure 1.

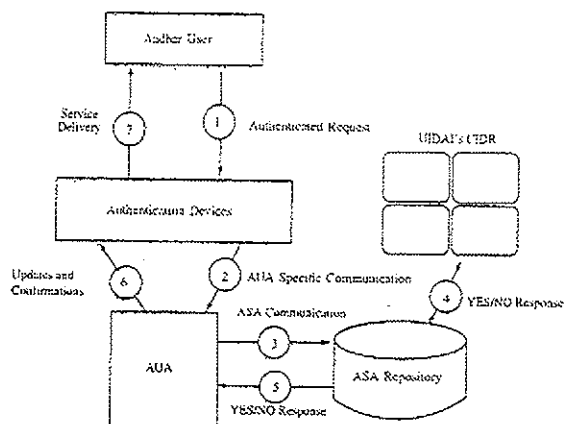


Fig. 1. The Aadhaar authentication framework (Figure inspired from (UIDAI, 2016b))

III. PRIVACY AND SECURITY IN AADHAAR: DEFINITIONS, ASSUMPTIONS AND REQUIREMENTS

In this section we do a requirement analysis for privacy and security. To begin, we provide some definitions.

A. Identity verification vs authentication

Aadhaar is a national identity project, but we believe that the subtle difference between identity verification and authentication is itself not well understood, and this leads to confusions in policy making and deployment. Below, we attempt to first demarcate the two concepts.

According to standard notions of digital authentication, a security principal (a user or a computer), while requesting access to a service, must provide two independent pieces of information - *identity* and *authentication*. Whereas identity provides an answer to the question "who are you?", authentication is a challenge-response process that provides a "proof of the claim of identity", typically using an authentication credential. Common examples of identity are User ID (Login ID), cryptographic public keys, email ids, ATM or smart cards;

some common authentication credentials are passwords (including OTPs), PINs and cryptographic private keys.

Identity may be considered public information but an authentication credential must necessarily be private - a secret that is known only to the user. Moreover, authentication must be a conscious process that requires active participation by a user, but not necessarily so for identity verification. As example use cases, a bank may want an identity verification while opening an account at which stage no secret like a password is usually necessary, but a user needs to authenticate with a PIN for transactions like ATM withdrawals. No publicly known information should be used as an authentication credential.

B. Privacy protection: fundamental assumptions

To determine the extent to which security and privacy are achieved, we must first define the desired expectations in this context. Our analysis is based on the following assumptions, which we believe are fundamental:

- 1) Authentication without consent should never be possible under any circumstances. Identification without consent should also not be possible except in some special situations like disaster management, identification of accident victims, law enforcement and such others. It should be noted that providing ones identity for obtaining services in any local context is always with consent.
- 2) Unapproved profiling, tracking and surveillance of individuals should not be possible. There should be sufficiently strong measures to prevent such breaches in privacy, with user-verifiable proof of the same.
- 3) The technical implementation of privacy and security must be provably correct with respect to the legal framework. The legal framework, in turn, needs to be suitably enhanced with special provisions to protect the privacy of individuals and society in an advanced information technology setting.

C. Possible ways of breach of privacy

In what follows we briefly examine the various ways in which the privacy of an individual can be compromised in a setting such as in Aadhaar.

- 1) *Correlation of identities across domains*: It may become possible to track an individual's activities across multiple domains of service (AUAs) using their global Aadhaar ids which are valid across these domains. This would lead to identification without consent.

173

- 2) *Identification without consent using Aadhaar data:* There may be unauthorised use of biometrics to illegally identify people. Such violations may include identifying people by inappropriate matching of fingerprint or iris scans or facial photographs stored in the Aadhaar database, or using the demographic data to identify people without their consent and beyond legal provisions.
- 3) *Illegal tracking of individuals:* Individuals may be tracked or put under surveillance without proper authorisation or legal sanction using the authentication and identification records and trails in the Aadhaar database, or in one or more AUA's databases. Such records will typically also contain information on the precise location, time and context of the authentication or identification, and the services availed.

We wish to emphasize that *insider attacks* are the most dangerous threats in this context. For instance, the second and third attacks above are much more likely if the attacker can collude with an insider with access to various components of the Aadhaar system.

D. Requirement analysis for privacy protection

In view of the above, effective privacy protection not only requires protecting the Aadhaar system from external attacks but from internal attacks as well. This requires strong guarantees on securing the data, logs and the transaction trails in the Aadhaar and the AUA systems. Specifically, one requires that:

- 1) UIDAI cannot be trusted against possible system hacks, insider leaks, and tampering of authentication records and audit trails. Indeed, the identity verification and authentication providing applications running on UIDAI computer systems should be trustworthy even when the UIDAI systems and the network cannot be trusted.
- 2) Manual inspection of user data, authentication records and audit trails should not be possible. In special cases of properly authorised investigations, such inspections may only be possible through pre-approved, audited and provably tamper proof computer programs, and an accurate tamper proof record of the entire investigation and digitally signed authorisation chain must be maintained at all times.
- 3) The enrolment agencies and the enrolment devices cannot be trusted from data privacy and security points of view; neither can the Point of Sale (POS) devices and various authentication user agencies

(AUAs), whether government or private, be trusted for data protection.

- 4) Authentication User Agencies (AUAs) cannot be trusted with biometric and demographic data; neither can they be trusted with sensitive user data of private nature (for example, medical and immunisation records etc.). All provisions of data privacy and security that apply to UIDAI, must also apply to the AUAs. Strong legal and policy frameworks are required to ensure this.
- 5) It should not be possible to correlate identities across application domains, except on suitably anonymised data through pre-approved, audited and provably tamper proof computer programs for carrying out data analysis.

In what follows we discuss the various threats and vulnerabilities that result from the Aadhaar project in more detail and analyse the measures adopted by the UIDAI against these. We also suggest a few possibilities of enhancing the privacy and security protections.

IV. AUTHENTICATION WITHOUT CONSENT

As we have already discussed, authentication without consent should not be possible under any circumstances. Additionally, it should be possible to revoke an authentication credential in case it is compromised, with the identity of the individual remaining intact.

UIDAI defines Aadhaar authentication as follows (UIDAI, 2016a): "*Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (demographic/biometrics/OTP) is submitted to UIDAI's Central Identities Data Repository (CIDR) for verification; the CIDR verifies whether the data submitted matches the data available in CIDR and responds with a Yes/No. No personal identity information is returned as part of the response*". (UIDAI, 2016a) goes on to define five types of Aadhaar based authentication:

- 1) *Type 1 Authentication:* Through this offering, service delivery agencies can use Aadhaar Authentication system for matching Aadhaar number and the demographic attributes (name, address, date of birth, etc) of a resident.
- 2) *Type 2 Authentication:* This offering allows service delivery agencies to authenticate residents through One-Time-Password (OTP) delivered to resident's mobile number and/or email address present in CIDR.
- 3) *Type 3 Authentication:* Through this offering, service delivery agencies can authenticate residents using one of the biometric modalities, either iris or fingerprint.

174

- 4) *Type 4 Authentication*: This is a 2-factor authentication offering with OTP as one factor and biometrics (either iris or fingerprint) as the second factor for authenticating residents.
- 5) *Type 5 Authentication*: This offering allows service delivery agencies to use OTP, fingerprint and iris together for authenticating residents.

A. Analysis of UIDAI measures

Thus, we see that authentication is implemented in Aadhaar via the mechanisms of passwords and biometric information. However, in the usage of biometrics, we believe there is an implicit confusion between the concepts of identity verification and authentication. In the above usage, biometric information is used for authentication relying on the unstated assumption that this information is private. However, we argue that biometric data is public: for instance, people's fingerprints can be lifted without their consent from a variety of objects that they may touch and their iris data may be picked up by a high resolution, directional camera from a distance. Even DNA information can be obtained from the objects that users may touch (Houck & Houck, 2008). Hence fraudulent presentation of biometric data for authentication, without conscious participation by a user, is a definite possibility (Akhtar, 2012).

Another difficulty with using biometrics as authentication credentials is that revoking biometrics like fingerprints or iris for a compromised user is problematic¹.

B. Possible remedies

The analysis in the prior section leads us to conclude that the usage of only biometrics in the context of Aadhaar authentication (type 3 authentication above) has significant problems. Type 1 authentication is susceptible to the same problem, since it also uses public information for authentication. It will be necessary to use other factors, like trustworthy manual oversight, in conjunction with these modalities for authentication. The other types use at least one private modality, and are hence safe.

We note that biometrics can certainly be very useful for identity verification. A careful case analysis must be performed to delineate whether identity verification or authentication is required in any given context, and UIDAI should appropriately change its authentication architecture to account for the above. Also, the legal and policy frameworks must make a clear distinction between authentication and identity verification.

¹We note that there is a notion of cancellable biometrics, but this is still in the research domain (Patei et al., 2015; Tulyakov et al., 2005) and may not yet integrate well with commercial matching software.

V. THE AADHAAR NUMBER AND THE POSSIBILITY OF IDENTIFICATION WITHOUT CONSENT

The Aadhaar number is at the heart of the Aadhaar scheme and is one of the biggest causes of concern. Recall that the Aadhaar number is a single unique identifier that must function across multiple domains. Given that the Aadhaar number must necessarily be disclosed for obtaining services, it becomes publicly available, not only electronically, but also often in human readable forms as well, thereby increasing the risk that service providers and other interested parties may be able to profile users across multiple service domains. Once the Aadhaar number of an individual is (inevitably) known, that individual may be *identified without consent* across domains, leading to multiple breaches in privacy as discussed in (Makkar, 2016; Centre for Internet & Society, 2016; The London School of Economics and Political Science, 2005).

Another worrisome issue is that of *identity theft*, whose potential for damage now increases manifold. As an illustrative example, let us consider the US Social Security Number (SSN) (Wikipedia, 2016s). The primary difference between Aadhaar and SSN is that the SSN does not have any biometric identifier attached and it does not support authentication. The SSN associated with a person provides a single interface to the person's dealings with a vast number of public and private bodies, very similar to how the usage of the Aadhaar number is being envisaged. While this facilitates use of administrative data for useful data analytics (Jennifer McNabb & Puckett, 2009), the ease of obtaining the SSN from across public and private databases also results in extremely high number of identity theft cases in the US (The London School of Economics and Political Science, 2005, page 100).

A. Analysis of UIDAI measures

The UIDAI does acknowledge the possibility of breach of privacy that can arise due to the use of a single identifier across multiple domains and recommends that the AUAs should use only domain specific identifiers in their dealings with people (UIDAI, 2011, page 7). Examples of domain specific identifiers are bank account numbers, passport numbers, driving license numbers, ration card numbers etc. The UIDAI mandates that the AUAs should maintain a mapping between their domain specific identifiers and the global Aadhaar numbers at their back-end. The UIDAI does not maintain any such mapping and assumes that there cannot be any breach of privacy from the UIDAI because the mappings are unidirectional.

175

This however does not fully mitigate the risks and the possibility of leakage of the Aadhaar number from an AUA, either from the database, or during "Know Your Customer" (KYC) processes, or even during availing services, cannot be ruled out. In particular, there appear to be no safeguards or even guidelines, either technical or legal, on how the Aadhaar number should be maintained and used by various AUAs in a cryptographically secure way, and how to prevent the Aadhaar number of an individual from becoming public. In fact, in many of the schemes that require Aadhaar authentication, it is necessary to provide the Aadhaar number as a public identifier. With such weak provisions, identification without consent and correlation of identities across application domains without approval remain as real possibilities. Additionally, since the Aadhaar number is supposed to be valid for life (UIDAI, 2011), it cannot easily be revoked in case of an identity theft or if the Aadhaar number is compromised in any other way.

B. Possible remedy

Thus, linking individuals across domains with a global identifier for legitimate data analysis, and the possible loss of privacy because of the correlation of identity across domains such a global identifier facilitates, are conflicting requirements. An alternative and more principled strategy to resolve the conflict would be for the UIDAI to issue different local identifiers (different Aadhaar numbers) for different domains, but to cryptographically embed in to all local identifiers a unique "master identifier". Several alternatives are possible. One may design the identifiers so that no linking across domains is possible at all, and it is impossible to isolate the global signature from any of the local identifiers. The linking then becomes unidirectional, but in the reverse direction to what UIDAI has currently suggested. Alternatively one may allow limited linking across domains, either bi-directional or even uni-directional. The LSE identity report actually suggests such a scheme (The London School of Economics and Political Science, 2005). Correlation across multiple domains using the master identifier, through cryptographically secure and pre-approved data analytics software, will always be possible in such a scheme. Sufficiently strong cryptographic measures should be used to embed the master identifier in to the local ones to prevent against possible external correlation attacks. Also, a major shift in the policy framework is necessary to reverse the direction of linking.

VI. PROTECTION OF USER DATA

In Section II we discussed that a major threat to privacy of users arises from the possibility of insider

attacks. In this section we discuss the possibilities of securing Aadhaar from such threats. While specifying the security requirement of a scheme such as Aadhaar - involving clients, service providers and an authentication agency - one can assume that the standard measures against external attacks like network firewalls, intrusion detection, hardware security modules (HSM), operating system hardening etc., will be incorporated by default.

A. Threat levels

In what follows, we outline the various levels of threat that are possible, and measures that can be taken in each case.

1) *Untrusted network, trusted application and authentication servers, trusted clients:* Among others, this scenario is common in internet banking, where the application and authentication servers are usually the same; in campus networks where snooping and attacks are fairly common; and in various internet and mobile application based services that use Google or Facebook for authentication. The basic security requirements in such situations are

- The authentication servers and the application servers must authenticate themselves to each other, and to the clients, to prevent against possible man-in-the-middle attacks (Wikipedia, 2016i).
- User credentials and other critical data must never travel over the network in unencrypted form.

Some commonly used solutions are provided by the encrypted version of the hypertext transfer protocol (HTTPS) (Wikipedia, 2016f) for accessing secure and signed web-pages, secure shell (SSH) (Wikipedia, 2016p) for establishing secure terminal sessions and virtual private networks (VPN) (Wikipedia, 2016v) for securely accessing an enterprise's private network from a remote location. All these protocols use encrypted tunnels through untrusted networks using techniques such as public key cryptography (PKI) (Wikipedia, 2016m), which enable the clients and the servers to verify the authenticity of other public servers, and possibly each other, before establishing secure encrypted communication channels. Kerberos (Wikipedia, 2016g) (also used in Microsoft Active Directory) based authentication and the Radius protocol (Wikipedia, 2016n) for WiFi are often used in campuses; and OAuth (Wikipedia, 2016l) is a common authentication and authorisation framework for public applications that use Google or Facebook for authentication. The client (access devices) and the servers themselves are assumed to be trusted and safe.

176

2) *Untrusted network, untrusted authentication and application servers, trusted clients*: This is a more challenging security situation where, in addition to the above, one also has to worry about data leaks from the servers, either due to hacking or even due to insider leaks. Some common counter measures are

- The authentication servers must never store any user credentials and may only store a Hash (Wikipedia, 2016c), a value computed from user credential(s) using a non-invertible function, and use it for matching. Then, user credentials can never leak.
- All critical data, records and logs must be stored only in encrypted forms on the servers. The decryption keys should not be easily accessible.
- There must be provisions for tamper detection for both data and programs.

Some of the common solutions are provided by cryptographic hashing techniques like *Secure Hash Algorithms (SHA-n)* (Wikipedia, 2016a,c), encryption techniques based on *Advanced Encryption Standard (AES)* (Wikipedia, 2016b) for protecting data, credentials and logs, *keyed-hash message authentication code (HMAC)* (Wikipedia, 2016e) based tamper detection, and hardware security modules (HSM) (Wikipedia, 2016d) for restricting insider access. These methods typically use symmetric key cryptography where the same key is used for both encryption and decryption. Challenge-response based authentication protocols like Kerberos (Wikipedia, 2016g) can ensure that the user credentials never travel over the network, even in encrypted format.

In even stricter situations, one may require in addition that

- The authentication servers must never store any information about user credentials, not even a hash.
- No process at the authentication servers should be able to glean any information whatsoever about user credentials from the information exchange during an authentication process.
- There are stronger guarantees for tamper detection. In particular,

- 1) The authentication and other servers must be able to prove to any designated auditor that they have not been tampered with and are running only pre-approved and inspected computer programs.
- 2) The servers must also be able to prove that none of their data, including records and log files, have been manually inspected or modified.

Advanced cryptographic measures may be used for such authentication (Wikipedia, 2016w; Sakashita et al.,

2009), although their usage is not common. Neither is it common to demand such strong tamper proof guarantees in most authentication and application systems. In Section VI-C we discuss some possibilities for such strong tamper protection guarantees.

3) *Untrusted clients*: In almost all internet applications, including banking, it is tacitly assumed that the client access devices - mobiles and handhelds, laptops and desktop computers - are trusted, and the responsibility of data protection in these devices are passed on to the users. However, in special situations where the access devices are not owned by the users but are provided by service providers, the users may have a right to be assured that data and credentials cannot be compromised from the access devices. Examples of such access devices are ATM machines, Aadhaar enrolment stations and other POS terminals. In all such cases one may require that:

- A client terminal or a POS device must be able to prove at all times to the server, and also to any approved third party auditor, that it has not been tampered with and does only what it is supposed to do.
- It should also be able to provide such a proof to a discerning user.

Later, in Section VI-C2 we discuss some possible solutions for securing such access devices.

B. Analysis of UIDAI measures

The security and privacy infrastructure of UIDAI has the following main features (UIDAI, 2014):

- 2048 bit PKI (Wikipedia, 2016m) encryption of biometric data in transit. End-to-end encryption from enrolment/POS to CIDR.
- Trusted network carriers (ASAs) between CIDR and AUAs. Effective precaution against denial of service (DOS) attacks.
- HMAC (Wikipedia, 2016e) based tamper detection of PID (Personal Identity Data) blocks, which encapsulate biometric and other data at the field devices.
- Registration and authentication of AUAs.
- Within CIDR only a SHA-n Hash (Wikipedia, 2016o) of Aadhaar number is stored.
- Audit trails are stored SHA-n encrypted (Wikipedia, 2016o), possibly also with HMAC (Wikipedia, 2016e) based tamper detection.
- Only hashes of passwords and PINs are stored. Biometric data are stored in original form though.
- Authentication requests have unique session keys and HMAC (Wikipedia, 2016e). Protection against

replay attacks.

- Resident data stored using 100 way sharding (vertical partitioning) (Wikipedia, 2016q). First two digits of Aadhaar number are used as shard keys.
- All enrolment and update requests link to partitioned databases using RefIDs (coded indices).
- All system accesses, including administration, through a hardware security module (HSM) (Wikipedia, 2016d) which maintains an audit trail.
- All analytics carried out only on anonymised data.

While these measures appear to be quite reasonable against external attacks, they may not be enough to forestall insider attacks. Though the safeguards adequately address the threat scenario described in Section VI-A1, they are not adequate for the threat levels described in Sections VI-A2 and VI-A3. For something as important as the national identity project, one will have to assume that the biggest security and privacy threats come from insider leaks. These include possible unauthorised and surreptitious examination of data, transaction records, logs and audit trails by personnel with access, leading to profiling and surveillance of targeted groups and individuals, perhaps at the behest of interested and influential parties in the state machinery itself. Hence, one would ideally like to have provisions to guard against the threat levels described in Section VI-A2 and Section VI-A3.

The following appear to be the main weaknesses:

- 1) Most of the security measures are based on cryptographic encryption techniques that require cryptographic keys to decode. Protection of these keys is of great importance, and it is necessary to have suitable measures to do so. Currently, we do not find mention of any such measures, and we believe that assuming trust in this context is a significant vulnerability. We do not believe that hardware security modules (HSM) (Wikipedia, 2016d), which are also under the administrative control of the same organisation, offer adequate protection against insider attacks for something as crucial as the national identity verification and authentication system.
- 2) There appears to be no well defined and cryptographically sound approval procedure for data inspection, whether for investigation or for analytics. This makes the system extremely open to abuse.
- 3) There appears to be no well defined procedure for audit and approval of various UIDAI programs and software. In particular, one would like to be able to establish that the programs have not been tampered with, and are doing precisely what they are supposed to do.

- 4) There appears to be no proper tamper detection and runtime audit of the field devices, including enrolment stations, to ensure that they are functioning true to specifications, and that there is no possibility of data leakage from the field devices.
- 5) Finally, we note that user biometric data are stored in the central repository, perhaps encrypted, but this still violates an important safeguard that we mentioned in Section VI-A2 - that user credentials should never be stored on the server. Unless there are some specific reasons to store the original biometric data it may be safer to store only non-invertible intermediate representations which are sufficient for matching (Tulyakov et al., 2005; Dodis et al., 2004).

C. Possible measures against insider attacks

Our starting point is that the environment in which the CIDR programs (code) are executed cannot be assumed as trusted. One must address the possibility that the attacker has full access to the computer programs that may be running on the UIDAI database. This may include both the source code and the run-time environment. How can one hope to secure such a system against insider attacks? We believe that two independent lines of defence are required:

- 1) There has to be an independent third party that can play the roles of an auditor and a keeper of cryptographic keys.
- 2) Several modern tools and techniques from computer science offer (partial) solutions to these problems. These need to be studied, evaluated and appropriately deployed.

In what follows we briefly describe each of these.

1) *Need for an independent third party:* Note that although critical data and transaction logs are maintained encrypted within the UIDAI, the decryption keys are also stored in the UIDAI systems. Since the decryption must happen routinely, the computer programs running in the UIDAI systems must be able to access these keys. There is no reason to believe that these keys cannot be retrieved with the collusion of multiple parties within the UIDAI in which case the data may be illegally accessed. The data may even be tampered and the HMAC (Wikipedia, 2016e) signatures recomputed without leaving a trail. Also, there is no way to guarantee that no unauthorised or tampered computer programs are running on the UIDAI systems. HSMs (Wikipedia, 2016d) under the same administrative control are not sufficient measures to engender confidence.

178

The problem appears to be unsolvable without the introduction of a completely independent third party, under a different administrative control, that can play the roles of a key-keeper and an auditor.

a) *Distributed key management.*: At least a part of every crucial decryption key must remain with the third party and a distributed key management protocol (Wikipedia, 2016h) must be put in place. The third party must programmatically share the portion(s) of the key(s) it holds with a corresponding computer program in the CIDR at run-time, through a cryptographically secure channel, only after authenticating the genuineness of the program using a cryptographic certificate and verifying that the program has not been tampered with.

b) *Audit and approval of UIDAI programs.*: To enable the above, it will be necessary for the auditor to examine, approve and cryptographically sign every program that may run in the CIDR. Thereafter, these programs should periodically during run-time and on demand, cryptographically prove to the auditor's programs that they are genuine and have not been tampered with.

c) *Audit of data inspection.*: All data inspection, including those through special purpose programs for data analytics, should be digitally approved by the auditor.

There has to be proper legal provisions for setting up such a third party audit and key-management system.

2) *Tools and techniques from computer science.*: Even with the above measures in place, the complete decryption keys will have to reside in the memory of the UIDAI computer systems at some point during the run-time. A well trained system administrator, with access to the hardware and the operating system, will still be able to access the decryption keys from the system's memory. There are a variety of tools in computer science that may provide a defence against such run-time attacks. We describe some of them below.

a) *Storing Hash of biometric data.*: Since the Aadhaar database stores sensitive biometric data of individuals, a useful strategy to protect this data is to store only a non-invertible hash of biometric data, which converts a string representing biometric data to a nearly uniform random string which does not leak any information about the individual. Some techniques to achieve these are *fuzzy extractor* (Dodis et al., 2004) and symmetric hashing (Tulyakov et al., 2005).

b) *Tamper-proof code.*: A significant cause of concern is that a malicious insider may be able to modify the code so that it behaves arbitrarily. Such attacks are dangerous not just in terms of denial of service, but also because arbitrary behaviour may lead to leakage of secrets embedded in code.

To address these attacks, one may use available techniques to transform code to *tamper-resistant* code (Wang et al., 2000; Michiels & Gorissen, 2007). Additionally, there are methods which prove the security and integrity of code without code transformations. Knowing that the behaviour of the server code does not change, one can resort to standard *static-code* analysis (Wikipedia, 2016i) and *model checking* techniques (Wikipedia, 2016j) in order to verify whether the server code works according to intended specifications. The behavioural specifications can be coded in known and industry-adopted formal executable languages (such as TLA+, Simulink/Stateflow, Message Sequence Charts, etc.). However, performing end-to-end static-code analysis or model checking on server code only addresses the question whether or not server code is acting maliciously. In the scenario when server code is established to be kosher, one has to still address the question of security when an adversary (read as environment or external user) tries to modify the code by cunningly exploiting the input interface of the server. A promising solution proposed in the security literature, which appears to be address the afore-mentioned problem is *control-flow integrity* (Martin Abadi, 2005). In a nutshell, this involves a runtime check on the code by installing an additional *monitor* which tracks the execution behaviour of the code and is aware of admissible behaviours of the program apriori. Third party audit will be required to set up the processes to ensure that the code is tamper free.

c) *Tamper-proof hardware.*: In addition to software solutions, tamper resistant hardware may also be leveraged for protection of cryptographic keys or data. For instance, servers in the presence of non-volatile memories can be subjected to side-channel attacks (Wikipedia, 2016r). Sensitive data that resides in memory across reboots can leak out to attackers. One way to secure a server's memory is to encrypt all memory transfers that take place between the processor cache onwards and the main memory. Encryption mechanisms as discussed in prior sections could be utilised for memory-transfer encryptions. A separate encryption controller unit would be mandated for this purpose.

Intel's Software Guard Extension (SGX) (Costan & Devadas, 2016) and its forerunners TPM and TXT (Wikipedia, 2016u) are yet another handy off-the-shelf solutions where protected areas (enclaves) of hardware are provided where execution of applications can take place without compromising BIOS, drivers, memory buses, and application's security. Furthermore, SGX also provide solutions for remote attestation challenges to ensure hardware integrity. Trusted hardware may be

179

leveraged to provide sought integrity and confidentiality. Here again, setting up and the safe-keep of the trusted hardware has to be entrusted to a third party organisation different from the UIDAI.

d) *Secure multi-party computation.*: Another method to secure keys or other private inputs is offered by the field of secure multi-party computation. Secure multi-party computation (Wikipedia, 2016k) is a field of cryptography that allows several mutually distrustful parties, each wishing to maintain privacy of their input data, to perform some computation on their joint data. This is a rich field with several efficient mechanisms in place to perform a large class of interesting computations privately. We believe that tools and techniques from this field may be relevant to the Aadhaar project: for instance, one may use a secret-sharing scheme to split the database across two servers belonging to different entities, ensuring that the two servers have disjoint sets of system administrators and diverse operating systems and hardware. This ensures that even if one server is hacked into, the data remains protected. Secure multiparty computation can be used to answer queries on the data distributed across servers.

e) *Homomorphic and functional encryption.*: Another security threat is the possibility of server breaches, whether the attack is launched from inside or outside the organisation. To prevent a server breach from leaking valuable user data, critical data needs to be stored on the server in encrypted form. However, encrypting data using standard methods leads to loss of functionality, such as the ability to perform data analytics. Recently, advanced forms of encryption have been designed by the cryptographic community that allow an untrusted server to compute on data "blind-folded". Two striking examples of such encryption mechanisms are the notions of homomorphic encryption (Gentry, 2009) and functional encryption (Sahai & Waters, 2005). At a high level, these systems allow sensitive data to be encrypted in a way that allows sophisticated computation on the data *in its encrypted form*. Thus, the functionality offered by data analytics can be enjoyed while ensuring privacy.

Such mechanisms may be very pertinent to ensuring privacy of data in the UIDAI database. However, while these systems are substantial achievements in cryptographic design, they remain far too slow for practical use. Nevertheless, for restricted classes of computations, such algorithms may be deployed. Third party intervention will be required to set up the computation in the encrypted domain.

f) *Symmetric Searchable Encryption and Extensions.*: Another method to perform useful computations

on encrypted data is offered by the field of symmetric searchable encryption, which enables searching on encrypted data (Bellare et al., 2007; Curtmola et al., 2011). Unlike notions such as functional encryption and homomorphic encryption described above, algorithms developed in the context of searchable encryption are highly efficient and scale well for massive sized data, such as the UIDAI data. For many investigative applications, tools and techniques developed in the context of searchable encryption appear to be very relevant.

g) *Whiteboxing and code obfuscation.*: Another useful class of defenses against insider attacks comes from techniques developed in the area of whitebox cryptography. Typically, one assumes that attacks are *blackbox*, i.e., an attacker has access to the input and the output of a program, but not to the internal workings of the program. However, an insider may have full access to the source code and binary file running on the system, and also the corresponding memory pages during execution. Additionally, the attacker can also possibly make use for debuggers and emulators, intercept system calls and tamper with the binary and its execution. Such attacks are called *whitebox* attacks, and whitebox cryptography (Preneel & Wyseur, 2008) aims to implement cryptographic procedures in software that transform and obfuscate code and data in such a way so that the cryptographic assets remain secure even when subject to whitebox attacks.

Although whitebox cryptography and obfuscation have been plagued with numerous attacks and there are impossibility results in theory for the general problem (Barak et al., 2001; Billet et al., 2004; Wyseur et al., 2007), successful whiteboxing in specific situations may well be possible (Delerablée et al., 2014; Bogdanov & Isobe, 2015). Many software packages that provide whitebox protection in restricted scenarios are available, and despite the lack of rigorous cryptographic guarantees, seem to work well in practice. Such packages may be deployed to enhance security against insider attacks. Note that the whitebox protection of security keys and the decryption code will have to be put in place by an independent third party.

D. Securing field devices

Finally, client access devices (or POS devices) can broadly be understood to have the same critical components that CIDR servers have: hardware (the device itself), and the application(s) running on the device. Solutions to secure client devices are no different than the solutions for servers that we discussed above.

Issue	Shortcoming in UIDAI measures	Key recommendations
Authentication without consent	Biometric and demographic data are public; hence, can be used without consent	- Demarcate identity verification and authentication. - Strengthen legal and policy frameworks See Sections III and IV for details.
Identification without consent using Aadhaar number	- Unidirectional linking from AUA-specific local ids to Aadhaar id. - No guidelines on safe maintenance of Aadhaar numbers by AUAs. - Vulnerable to correlation of identity across domains.	- Unidirectional linking from Aadhaar id to AUA-specific ids - Cryptographically embed Aadhaar id into AUA-specific ids making correlation impossible See Section V for details.
Unlawful access of CIDR data leading to profiling, tracking and surveillance	- Inadequate protection against insider attacks on CIDR data - CIDR data encrypted but the decryption keys reside in CIDR - UIDAI human managers can have access to decryption keys	- Separate administrative control for on-line audit and key management - Legal framework for the above - Only hashes of Biometric data must be stored on servers. - Manual inspection of CIDR data must not be possible - Only pre-approved and audited computer programs with tamper-proof guarantees should access CIDR data - All investigations and analyses only with prior audit and approval through pre-approved computer programs - Tamper proof guarantees for field devices - Adopt modern tools from computer science to implement the above protections See Section VI for details.

TABLE I
SUMMARY OF OUR ANALYSIS AND RECOMMENDATIONS

VII. CONCLUSIONS

We have analysed the Aadhaar project from the points of view of privacy and security and have pointed out some technical weaknesses and possible remedies. Specifically, we have found that

- 1) The Aadhaar number, which is a single global identifier that is supposed to work across application domains, makes individuals vulnerable to privacy breaches. A design alteration can however make it safe.
- 2) The slightly different concepts of authentication and identity verification need to be well demarcated, and careful use case analysis is required to determine precisely what is required for each application. The legal framework must also make note of these.
- 3) In an Aadhaar like setup, the biggest threat to privacy comes from potential insider leaks. The Aadhaar technology architecture does not seem to have been explicitly designed to have strong protections against such insider leaks. We believe that effective protection against insider leaks necessarily requires a third party auditor under independent

administrative control. With such a provision in place there are several tools from computer science that can provide reasonable guarantees for security and privacy protection.

We summarise our analysis and key findings in Table I.

Thus, though there are serious privacy concerns at present, we believe that Aadhaar can be made safe from a technology perspective with due-diligence. The legal framework however needs to be more specific and requires significant strengthening. Perhaps the single most important specific question that begs answering is *who should have the right to verify the identity of an individual, and under what circumstances?* Above all, we believe that the Aadhaar project requires informed and comprehensive policy debates, covering all angles, to realise its full effectiveness without causing the kind of disruptions that have been reported.

The effectiveness of biometric identification and to what extent are the biometric features required are remaining important questions that require further study.

181

ACKNOWLEDGEMENT

We thank Reetika Khera for the many discussions, and Ambuj Sagar and Narayanan Kurur for suggestions on improving our manuscript. The first author thanks Manoj Prabhakaran for many helpful comments and Mihir Bellare for suggesting the use of fuzzy extractors.

REFERENCES

- Akhtar, Zahid. 2012 (March). Security of Multimodal Biometric Systems against Spoof Attacks. Ph.D. thesis. Dept. of Electrical and Electronic Engineering, University of Cagliari. http://pralab.diee.unica.it/sites/default/files/Akhtar_PhD2012.pdf.
- Arun, Chinmayi. 2016. Privacy is a fundamental right. <http://www.thehindu.com/opinion/lead/lead-article-on-aadhaar-bill-by-chinmayi-arun-privacy-is-a-fundamental-right/article8366413.ece>. [Online; posted 18-March-2016].
- Athey, Susan, & Imbens, Guido W. 2015 (April). Machine Learning for Estimating Heterogeneous Casual Effects. Tech. rept. Stanford University. <https://www.gsb.stanford.edu/faculty-research/working-papers/machine-learning-estimating-heterogeneous-casual-effects>.
- Barak, Boaz, Goldreich, Oded, Impagliazzo, Russell, Rudich, Steven, Sahai, Amit, Vadhan, Salil, & Yang, Ke. 2001. On the (im) possibility of obfuscating programs. Pages 1–18 of: Annual International Cryptology Conference. Springer.
- Bellare, Mihir, Boldyreva, Alexandra, & O'Neill, Adam. 2007. Deterministic and efficiently searchable encryption. Pages 535–552 of: Annual International Cryptology Conference. Springer.
- Bhatia, Gautam. 2015. Sorry, Mr. Attorney-General, We Do Actually Have a Constitutional Right to Privacy. <http://thewire.in/2015/07/28/sorry-mr-attorney-general-we-do-actually-have-a-constitutional-right-to-privacy-7398/>. [Online; posted 28-July-2015].
- Billet, Olivier, Gilbert, Henri, & Ech-Charbi, Charaf. 2004. Cryptanalysis of a white box AES implementation. Pages 227–240 of: International Workshop on Selected Areas in Cryptography. Springer.
- Bogdanov, Andrey, & Isobe, Takanori. 2015. White-Box Cryptography Revisited: Space-Hard Ciphers. Pages 1058–1069 of: Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15. New York, NY, USA: ACM.
- Centre for Internet & Society, The. 2016. List of Recommendations on the Aadhaar Bill, 2016 - Letter Submitted to the Members of Parliament. <http://cis-india.org/internet-governance/blog/list-of-recommendations-on-the-aadhaar-bill-2016>. [Online; posted 16-March-2016].
- Costan, Victor, & Devadas, Srinivas. 2016. Intel SGX Explained. IACR Cryptology ePrint Archive, 2016, 86.
- Curtmola, Reza, Garay, Juan, Kamara, Seny, & Ostrovsky, Rafail. 2011. Searchable symmetric encryption: improved definitions and efficient constructions. Journal of Computer Security, 19(5), 895–934.
- Delerablée, Cécile, Lepoint, Tancrède, Paillier, Pascal, & Rivain, Matthieu. 2014. White-Box Security Notions for Symmetric Encryption Schemes.
- Diffie, Whitfield, & Hellman, Martin E. 1979. Privacy and Authentication: An Introduction to Cryptography. Proceedings of the IEEE, 67(March), 397–427. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1455525>.
- Dodis, Yevgeniy, Reyzin, Leonid, & Smith, Adam. 2004. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Pages 523–540 of: International Conference on the Theory and Applications of Cryptographic Techniques. Springer.
- Drèze, Jean. 2016. The Aadhaar coup. <http://www.thehindu.com/opinion/lead/jean-dreze-on-aadhaar-mass-surveillance-data-collection/article8352912.ece>. [Online; posted 15-March-2016].
- Duggal, Pavan. 2011. Does the UID project infringe on privacy? http://www.business-standard.com/article/opinion/does-the-uid-project-infringe-on-privacy-111080300006_1.html. [Online; posted 3-August-2011].
- Einav, Liran, & Levin, Jonathan. 2014. Economics in the age of big data. Science, 346(6210), <http://science.sciencemag.org/content/346/6210/1243089>.
- Einav, Liran, & Levin, Jonathan D. 2013 (May). The Data Revolution and Economic Analysis. Working Paper 19035. National Bureau of Economic Research. <http://www.nber.org/papers/w19035>.
- Express News Service. 2016. Aadhar Bill passed in Lok Sabha, Opposition fears surveillance. <http://indianexpress.com/article/india/india-news-india/aadhar-card-uid-bill-lok-sabha-arun-jaitley/>. [Online; posted 12-March-2016].
- Gentry, Craig. 2009. Fully homomorphic encryption using ideal lattices. Pages 169–178 of: STOC.
- Houck, Max, & Houck, Lucy. 2008 (August). What is touch DNA? <http://www.scientificamerican.com/article/experts-touch-dna-jonbenet-ramsey/>. [Online; posted 28-July-2015].
- Jayaram, Malavika. 2015. Aadhaar debate: Privacy is not an elitist concern it's the only way to secure equality. <http://scroll.in/article/748043/aadhaar-debate-privacy-is-not-an-elitist-concern-its-the-only-way-to-secure-equality>. [Online; posted 15-August-2015].
- Jennifer McNabb, David Timmons, Jae Song, & Puckett, Carolyn. 2009. Uses of Administrative Data at the Social Security Administration. Social Security Bulletin, 16. <https://www.ssa.gov/policy/docs/ssb/v69n1/v69n1p75.html>.
- Johari, Aarefa. 2016. In drought-hit Saurashtra, poor internet network can often mean no food rations. <http://scroll.in/article/810683/in-drought-hit-saurashtra-no-internet-can-often-mean-no-food-rations>. [Online; posted 26-June-2016].
- Khera, Reetika. 2011. The UID Project and Welfare Schemes. Economic and Political Weekly, Vol. 46(Issue No. 09).
- Khera, Reetika. 2013. Lessons from the East Godavari pilot. <http://www.thehindu.com/opinion/lead/lessons-from-the-east-godavari-pilot/article4603273.ece>. [Online; posted 11-April-2013].
- Khera, Reetika. 2015. Five Myths about Aadhar. <http://www.outlookindia.com/website/story/five-myths-about-aadhar/295364>. [Online; posted 18-September-2015].
- Kleinberg, Jon, Ludwig, Jens, Mullainathan, Sendhil, & Obermeyer, Ziad. 2015. Prediction Policy Problems. American Economic Review, 105(5), 491–95. <http://www.aeaweb.org/articles?id=10.1257/aer.p20151023>.

- Krishnamurthy, Rashmi, & Desouza, Kevin C. 2014. Big Data Analytics: The Case of Social Security Administration. *Information Policy*, 19(May), 165–178. <http://ssrn.com/abstract=2757871>.
- Kumar, Ashwani. 2015. Privacy, a non-negotiable right. <http://www.thehindu.com/opinion/lead/privacy-a-nonnegotiable-right/article7519148.ece>. [Online; posted 10-August-2015].
- Lok Sabha Secretariat: New Delhi. 2012. Report by the Parliamentary Standing Committee on Finance (2011-2012) chaired by Shri Yashwant Sinha. http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.
- Makkur, Sahil. 2016. Aadhaar is actually surveillance tech: Sunil Abraham. http://www.business-standard.com/article/opinion/aadhaar-is-actually-surveillance-tech-sunil-abraham-116031200790_1.html. [Online; posted 12-March-2016].
- Martin Abadi, Mihai Budiu, Úlfar Erlingsson Jay Ligatti. 2005 (nov). Control-Flow Integrity. Pages 340–353 of: *ACM Conference on Computer and Communication Security (CCS)*.
- Masiéro, Silvia. 2015. PDS computerisation: What other states can learn from Kerala. http://www.ideasforindia.in/article.aspx?article_id=1474. [Online; posted 6-July-2015].
- McBride, Linden, & Nichols, Austin. 2015 (January). Improved poverty targeting through machine learning: An application to the USAID Poverty Assessment Tools. Tech. rept. Economics That Really Matters, Charles H. Dyson School of Applied Economics and Management at Cornell University. http://www.econthatmatters.com/wp-content/uploads/2015/01/improvedtargeting_21jan2015.pdf.
- Mehta, Pratap Bhanu. 2016. Privacy after Aadhaar. <http://indianexpress.com/article/opinion/columns/privacy-after-aadhaar-money-bill-rajya-sabha-upa/>. [Online; posted 26-March-2016].
- Michiels, W., & Gorissen, P. 2007. Mechanism for Software Tamper Resistance: An Application of White-box Cryptography. In: *Proceedings of the 2007 ACM Workshop on Digital Rights Management, DRM '07*.
- NDTV. 2016a. Truth vs Hype: Aadhaar's One Billion Challenge. <http://www.ndtv.com/video/news/truth-vs-hype/truth-vs-hype-aadhaar-s-one-billion-challenge-411279>. [Online; posted 9-April-2016].
- NDTV. 2016b. What should they do who dont get ration. <http://khabar.ndtv.com/video/show/ndtv-special-ndtv-india/what-should-they-do-who-dont-get-ration-423998>. [Online; posted 16-July-2016].
- Patel, V. M., Ratha, N. K., & Chellappa, R. 2015. Cancelable Biometrics: A review. *IEEE Signal Processing Magazine*, 32(5), 54–65.
- Preneel, Bart, & Wyseur, Brecht. 2008. White-Box Cryptography.
- PTI. 2015. Right to Privacy not a fundamental right, cannot be invoked to scrap Aadhar: Centre tells Supreme Court. http://articles.economictimes.indiatimes.com/2015-07-23/news/64773078_1_fundamental-right-attorney-general-mukul-rohategi-privacy. [Online; posted 23-July-2015].
- Sahai, Amit, & Waters, Brent. 2005. Fuzzy Identity-Based Encryption. Pages 457–473 of: *EUROCRYPT*.
- Sakashita, Taiki, Shibata, Yoichi, Yamamoto, Takumi, Takahashi, Kenta, Ogata, Wakaba, Kikuchi, Hiroaki, & Nishigaki, Masakatsu. 2009. A Proposal of Efficient Remote Biometric Authentication Protocol. Berlin, Heidelberg: Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-04846-3_14. Pages 212–227.
- Scroll Staff. 2016. Jaitley admits right to privacy but brazens it out on Money Bill manoeuvre for Aadhaar. <http://scroll.in/article/805236/jaitley-admits-right-to-privacy-but-brazens-it-out-on-money-bill-manoevr-for-aadhar>. [Online; posted 16-March-2016].
- The London School of Economics and Political Science. 2005 (June). The Identity Project: An assessment of the UK Identity Cards Bill and its implications. <http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf>.
- The Planning Commission: Government of India. 2011 (December). Report of the Group of Experts on Privacy chaired by Justice A P Shah. http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.
- Tulyakov, Sergey, Farooq, Faisal, & Govindaraju, Venu. 2005. Symmetric Hash Functions for Fingerprint Minutiae. Berlin, Heidelberg: Springer Berlin Heidelberg. Pages 30–38.
- UIDAI. 2011. Aadhaar Security Policy & Framework for UIDAI Authentication (Version 1.0). http://uidai.gov.in/images/authDoc/d3_4_security_policy_framework_v1.pdf. [Online; accessed 31-July-2016].
- UIDAI. 2014. AADHAAR TECHNOLOGY & ARCHITECTURE: Principles, Design, Best Practices, & Key Lessons. https://uidai.gov.in/images/AadhaarTechnologyArchitecture_March2014.pdf. [Online; accessed 31-July-2016].
- UIDAI. 2016a. Authentication Overview. <https://uidai.gov.in/auth.html>. [Online; accessed 31-July-2016].
- UIDAI. 2016b. Operating Model Overview. <https://uidai.gov.in/authentication-2/operation-model.html>. [Online; accessed 31-July-2016].
- UN Global Pulse. 2012 (May). Big Data for Development: Challenges and Opportunities. <http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseMay2012.pdf>.
- UN Global Pulse. 2016 (August). Data for Development: Challenges and Opportunities. <http://www.unglobalpulse.org/>. [Online; accessed 7-August-2016].
- Varian, Hal R. 2014. Big Data: New Tricks for Econometrics. *Journal of Economic Perspectives*, 28(2), 3–28. <http://www.aeaweb.org/articles?id=10.1257/jep.28.2.3>.
- Vombatkere, Sudhir. 2016. How Aadhaar Neglects Personal Privacy and National Security. *Mainstream, LIV No 13*(March). <http://www.mainstreamweekly.net/article6283.html>. [Online; posted 15-August-2015].
- Wang, Chenxi, Hill, Jonathan, Knight, John, & Davidson, Jack. 2000. Software Tamper Resistance: Obstructing Static Analysis of Programs. Tech. rept. Charlottesville, VA, USA.
- Wikipedia. 2016a. Aadhaar. <https://en.wikipedia.org/wiki/Aadhaar>. [Online; accessed 31-July-2016].
- Wikipedia. 2016b. Advanced Encryption Standard. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Online; accessed 30-July-2016].
- Wikipedia. 2016c. Cryptographic hash function. https://en.wikipedia.org/wiki/Cryptographic_hash_function. [Online; accessed 30-July-2016].

183

- Wikipedia. 2016d. Hardware security module. https://en.wikipedia.org/wiki/Hardware_security_module. [Online; accessed 30-July-2016].
- Wikipedia. 2016e. Hash-based message authentication code. https://en.wikipedia.org/wiki/Hash-based_message_authentication_code. [Online; accessed 30-July-2016].
- Wikipedia. 2016f. HTTPS. <https://en.wikipedia.org/wiki/HTTPS>. [Online; accessed 30-July-2016].
- Wikipedia. 2016g. Kerberos (protocol). [https://en.wikipedia.org/wiki/Kerberos_\(protocol\)](https://en.wikipedia.org/wiki/Kerberos_(protocol)). [Online; accessed 30-July-2016].
- Wikipedia. 2016h. Key management. https://en.wikipedia.org/wiki/Key_management. [Online; accessed 30-July-2016].
- Wikipedia. 2016i. Man-in-the-middle attack. https://en.wikipedia.org/wiki/Man-in-the-middle_attack. [Online; accessed 30-July-2016].
- Wikipedia. 2016j. Model Checking. https://en.wikipedia.org/wiki/Model_checking.
- Wikipedia. 2016k. MPC. https://en.wikipedia.org/wiki/Secure_multi-party_computation.
- Wikipedia. 2016l. OAuth. <https://en.wikipedia.org/wiki/OAuth>. [Online; accessed 30-July-2016].
- Wikipedia. 2016m. Public key infrastructure. https://en.wikipedia.org/wiki/Public_key_infrastructure. [Online; accessed 30-July-2016].
- Wikipedia. 2016n. RADIUS. <https://en.wikipedia.org/wiki/RADIUS>. [Online; accessed 30-July-2016].
- Wikipedia. 2016o. Secure Hash Algorithm. https://en.wikipedia.org/wiki/Secure_Hash_Algorithm. [Online; accessed 30-July-2016].
- Wikipedia. 2016p. Secure Shell. https://en.wikipedia.org/wiki/Secure_Shell. [Online; accessed 30-July-2016].
- Wikipedia. 2016q. Shard (database architecture). [https://en.wikipedia.org/wiki/Shard_\(database_architecture\)](https://en.wikipedia.org/wiki/Shard_(database_architecture)). [Online; accessed 30-July-2016].
- Wikipedia. 2016r. Side-channel attack. https://en.wikipedia.org/wiki/Side-channel_attack. [Online; accessed 31-July-2016].
- Wikipedia. 2016s. Social Security Number. https://en.wikipedia.org/wiki/Social_Security_number. [Online; accessed 31-July-2016].
- Wikipedia. 2016t. Static program analysis. https://en.wikipedia.org/wiki/Static_program_analysis.
- Wikipedia. 2016u. Trusted Execution Technology. https://en.wikipedia.org/wiki/Trusted_Execution_Technology.
- Wikipedia. 2016v. Virtual Private Network. https://en.wikipedia.org/wiki/Virtual_private_network. [Online; accessed 30-July-2016].
- Wikipedia. 2016w. Zero-knowledge proof. https://en.wikipedia.org/wiki/Zero-knowledge_proof. [Online; accessed 30-July-2016].
- Wyseur, Brecht, Michiels, Wil, Gorissen, Paul, & Preneel, Bart. 2007. Cryptanalysis of white-box DES implementations with arbitrary external encodings. Pages 264–277 of: International Workshop on Selected Areas in Cryptography. Springer.
- Yadav, Anumecha. 2016a (April). Rajasthan presses on with Aadhaar after fingerprint readers fail: Well buy iris scanners. <http://scroll.in/article/806245/rajasthan-presses-on-with-aadhaar-after-fingerprint-readers-fail-well-buy-iris-scanners>. [Online; posted 10-April-2016].
- Yadav, Anumecha. 2016b (August). Rajasthans living dead: Thousands of pensioners without Aadhaar or bank accounts struck off lists. <http://scroll.in/article/813132/rajasthans-living-dead-thousands-of-pensioners-without-aadhaar-or-bank-accounts-struck-off-lists>. [Online; posted 6-August-2016].
- Zhong, Raymond. 2016. Is the Indian Government Saving as Much as It Says on Gas Subsidies?. <http://blogs.wsj.com/indiarealtime/2016/03/21/is-the-indian-government-saving-as-much-as-it-says-on-gas-subsidies/>. [Online; posted 21-March-2016].

IN THE SUPREME COURT OF INDIA
CIVIL ORIGINAL JURISDICTION
TRANSFER CASE (CIVIL) NO. 152 OF 2013

88 104
Annexure R-5

Vickram Crishna & Ors.

... Petitioners

Versus

UIDAI & Ors.

... Respondents

AND

WRIT PETITION (CIVIL) NO. 797 OF 2016

S.G. Vombatkere & Anr.

... Petitioners

Versus

Union of India & Ors.

... Respondents

SUBMISSIONS OF MS. MEENAKSHI ARORA, SR. ADV.
ON BEHALF OF THE PETITIONERS

Introduction

- A. By way of the aforementioned Petitions, the Petitioners have challenged the constitutional validity of the Aadhaar Project including the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter "**the Act**"), various Regulations issued thereunder (including the Aadhaar (Enrolment and Update) Regulations, 2016 (hereinafter "**the Enrolment Regulations**") and the Aadhaar (Authentication) Regulations, 2016 (hereinafter "**the Authentication Regulations**") as well as the several notifications and circulars purported to be issued for the implementation of the Act.
- B. It may be recalled that the Aadhaar Project has been projected as a "*unique identity project*" with the avowed intention of "*providing*" an identity to every resident of India.
- C. To this end, the Aadhaar Project contemplates creation of a "*single source of truth*":
- Assignment of a 16-digit number linked with the identity information (i.e. demographic and biometric information) to all residents, so as to provide for a "*unique identity*";
 - Identity information so collected is stored with the Central Identities Data Repository (hereinafter "**the CIDR**");
 - A resident is required to *prove* his/ her identity by authentication of the data available *inter alia* by means of biometric authentication through a device which is linked to the CIDR database which matches the same in order to determine whether the person is who he or she claims to be;
 - CIDR retains authentication records (detailed hereinafter), including the *meta data* associated with the authentication.
 - An ever-increasing number of services, benefits and subsidies are made contingent entirely upon obtaining an Aadhaar Number and being authenticated by a biometric based system or through a one-time password (hereinafter, "**OTP**").
 - Aadhaar is being compulsorily seeded/ linked with all databases. This is being done by organic seeding i.e. with the active consent of the parties or through inorganic

68/185

reasonable nexus between stringency of the provision and the purpose sought to be achieved ceases to exist.

33. In the present case, with rapid advances in technology, it is not foreseeable as to what uses the data of an individual could be put to in the future or what impact enrolment could have on her or how the law could be used against her. The reality of this assertion has been recognized in *Puttaswamy*, by this Hon'ble Court at ¶ 300-305.

34. In these circumstances, there is a legitimate and serious apprehension of misuse and abuse of the data collected, and the mere existence of the Project which makes this possible is sufficient ground to request the Court to quash the same. In light of the above, and given the chilling effect this has on free exercise of fundamental rights, a person cannot be compelled to enrol under the Aadhaar Project.

V. **THE AADHAR PROJECT LACKS SAFEGUARDS FOR DATA PROTECTION AND SECURITY, AND HENCE AMOUNTS TO A VIOLATION OF OBLIGATIONS OF STATE UNDER PART III OF THE CONSTITUTION OF INDIA, INCLUDING TO PROTECT THE RIGHT TO LIFE, LIBERTY, DIGNITY AND PRIVACY OF EVERY PERSON.**

35. It is beyond any cavil of doubt that it is the duty and responsibility of the State to ensure that the Right to Life, Liberty, Dignity and Privacy of every person is not breached. It is therefore not open to the State either to directly, or through private entities cause breach of such rights, which it is mandated to protect. The protection must necessarily extend to the Personal Data of such persons, in particular that which has been collected by or, at the instance of the State.

36. In this context, it would be instructive also see *Tele2* wherein it was held that:

122. ... Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period

Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

37. The German FCC Judgment struck down the law *inter alia* for lacking a high standard of data security and privacy, as follows:

"In contrast, the guarantee of a particularly high standard of security, which is constitutionally necessary for such a data pool, is missing. In this respect, § 113a.10 TKG only provides the duty, which remains undefined, to ensure by technical and organisational measures that access to the stored data is possible solely for persons who are specially authorised, and apart from this refers only to the care which is necessary in general in the area of telecommunications. There is therefore no provision which takes account of the particularly strict standards required of the security of the extensive and informative data pool under § 113a TKG. §§ 88 and 109 TKG, which are referred to with regard to their contents, do

86

not guarantee such a particularly high security standard, but permit a wide range of relative degrees, corresponding to their wide area of application....

Nor is it ensured by statutory orders or by orders of the regulatory authorities that these standards are put into specific terms. In particular, § 110 TKG does not guarantee that adequate security standards apply. Admittedly, the delegated legislation to be passed under this statute (see § 110.2 and 3 TKG) may include aspects of data security. However, this statute – which is primarily determined by technical objectives – neither contains substantive standards, nor does it otherwise take up the aspect of data security. Apart from this, even two years after the duty of storage of § 113a TKG entered into force, the Telecommunications Interception Order (Telekommunikationsüberwachungsverordnung – TKÜV) has not been adapted to take account of the reform of the law.” (para 271)

“All in all, therefore, there is no guarantee in a binding form and in well-defined provisions of a particularly high security standard for the data to be stored under § 113a TKG. Neither are the instruments cited by the experts in the present proceedings as central elements (separate storage, asymmetric encryption, the four-eyes principle in conjunction with advanced authentication procedures for access to the keys, revision-proof recording of access and deletion) imposed on the persons with a duty of storage in an enforceable manner, nor are other precautions which guarantee a comparable level of security imposed on them. Nor is there a balanced system of sanctions that attributes no less weight to violations of data security than to violations of the duties of storage themselves. The range of administrative fines for non-compliance with the duties of storage is markedly broader than that for the violation of data security... The current legal situation therefore does not satisfy the constitutional requirements of the security of a data pool as is created by § 113a TKG.” (para 275)

(Emphasis supplied)

38. The U.N. Human Rights Council, in its Resolution on the Right to Privacy in the Digital Age²¹ dated 22 March 2017, has specifically expressed its concern as to the fact that:

“... individuals often do not provide their free, explicit and informed consent to the re-use, sale or multiple re-sales of their personal data, as the collecting, processing and sharing of personal data, including sensitive data, has increased significantly in the digital age...”

39. In the instant case, there is no provision for effective security of the data aggregated under the Aadhar Project:

²¹ The Resolution took note of the following:

- a. Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression. U.N. Doc. A/HRC/23/40 (17 April 2013), wherein the Special Rapporteur has opined that:
 77. States must ensure that the private sector is able to carry out its functions independently in a manner that promotes individuals' human rights. At the same time, corporate actors cannot be allowed to participate in activities that infringe upon human rights, and States have a responsibility to hold companies accountable in this regard...
 96. States must refrain from forcing the private sector to implement measures compromising the privacy, security, and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption
- b. Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression. U.N. Doc. A/HRC/29/32 (22 May 2015), wherein the Special Rapporteur has opined at ¶ 55 that:
 Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. **A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.**

- a. The Act contains no provisions for data protection, apart from a mere obligation on the Authority to ensure security of the information (*See*: S. 28). Even that is pitifully vague and fails to lay down any standard of data security or prescribe any cogent measures which are to be taken to prevent data breaches.
- b. While the Authority is empowered to prescribe, by way of Regulations, the process *inter alia* for maintaining data security [S. 54(2)(p)], the Aadhar (Data Security) Regulations, 2016 simply vests in the Authority a discretion to specify “an information security policy” [Reg. 3]. Till date, no such policy has been laid down.
- c. At any rate, Regulation 3, which vests in UIDAI the discretion to notify a policy regarding data security amounts to excessive delegation of power and hence cannot be sustained.

In this regard, without prejudice to the argument that the Act is *per se* bad for over-delegation, it is respectfully submitted that Regulations prepared pursuant to Section 54 is subject to Parliamentary oversight, unlike policies prepared by the UIDAI. Since Section 54(2)(p) contemplated preparation and notification of data protection regulations by the UIDAI, it necessarily contemplated making the same subject to Parliamentary oversight. It is therefore not open to the UIDAI to exclude such oversight by vesting unto itself the discretion to issue policies in this regard.

- d. Further, while the servers of the Requesting Entity and the ASA are required to be located in data centres in India [Regulation 22(1), Authentication Regulations], there is no such requirement for the CIDR itself, which is the centralized database with all data. Rather, S. 2(h) of the Act, which defines CIDR, only provides that it is a “centralised database in one or more locations....”.
40. In the absence of effective protective measures in place, it is not open to the State to insist on a compulsory acquisition of personal data of the entire population.
 41. Further, the Project itself provides for access to the personal data by various private entities e.g. AUAs, KUAs and other private entities (such as the banks, insurance companies and telecom service providers), who are entitled to access an individual’s information linked to her Aadhaar number.
 42. The periodic reports of UIDAI data breaches establishes the vulnerability of the system and the capability of cyber attackers. Given the nature and vulnerability of data available with the CIDR, it could act as a kill switch in the hands of any person/state inimically disposed towards India. Such catastrophe would neither give our Nation an alternative remedy nor Courts to then consider the consequences of collecting and putting into one bucket all this succulent information of the Nation’s individuals. Through information warfare and cyber terrorism, terrorists and foreign governments can accomplish their political objectives without firing a physical bullet.
 43. The collation of sensitive personal data and / or information of all residents of India in a centralized database is inadvertently exposing India to the growing threat that cyber warfare poses in today’s world. Till date there is no policy, strategy or official methodology to pre-empt, deal with, tackle, and / or remedy a cyber-attack on critical national infrastructure such as an attack on the CIDR.
 44. In this regard, it may be noted that:
 - a. larger the number of entities which have access to or the ability to store the data, the more difficult it becomes to maintain the privacy and confidentiality thereof and prevent breaches and leakages.

- b. The laws struck down in *Tele2* and the German FCC Judgement required data to be collected and stored by private parties.
- c. Under the Aadhaar Project, this information can be easily accessed even by private entities and exploited for commercial gain. Reference in this regard may be had to the submissions in I.A. No. _____ of 2018 in Writ Petition No. 494 of 2012 for intervention *inter alia* by Digital Lenders Association of India & Ors. wherein it has been admitted by Handy Online Solutions Pvt. Ltd. (Applicant No. 5 therein) that:

24. ... *It uses the Aadhaar system to provide quick and reliable verification of the identity of persons in need of employment...*

25. ... *Further, even if they have any other proof of identification such as driving license, ration cards or voter ID cards etc., verification is difficult without the Aadhaar system since other databases may be valid only within the domiciliary state, may not be up-to-date or have all the relevant information...*

- d. Admittedly, private companies have developed mobile phone applications, such as OnGrid, that enable background checks on persons using the Aadhaar platform as a base [see p. 4, Module VII-D]. Such commercialization of personal and private data of people is evident from the aforementioned application admitting that they have '*developed innovative business models that are dependent on the existence of the Aadhaar system*' and that '*there are several persons and businesses who depend on the Aadhaar system*'. They further state that '*The business model of the Applicants is dependent upon the existence and implementation of the Aadhaar system in its current legislative framework. Any order passed in the captioned Writ Petition or its connected matters will affect the Applicants' businesses and commercial interests...*'
- e. Further, admittedly, SRDHs have already built comprehensive databases containing information far in excess of what is required under the Aadhaar Act. This database is available to private entities for purposes such as targeting potential customers etc.²²

45. Thus, apart from failing to provide for appropriate provisions to ensure protection of the rights of the individuals, the State has actively indulged in commercialization of such private data, representing an abject failure to meet its obligations under Part III of the Constitution of India.

VI. THE AADHAR PROJECT LACKS JUDICIAL SAFEGUARDS AND EFFECTIVE REMEDIES IN THE EVENT OF BREACH

46. In *Szabó*, the Court held as follows:

39. *Considering in addition that the domestic law does not appear to provide any possibility for an individual who alleges interception of his or her communications to lodge a complaint with an independent body, the Court is of the view that the applicants can claim to be victims of a violation of their rights under the Convention, within the meaning of Article 34 of the Convention.*

75. *A central issue common to both the stage of authorisation of surveillance measures and the one of their application is the absence of judicial supervision. The measures are authorised by the Minister in charge of justice upon a proposal from the executives of the relevant security services, that is, of the TEK which, for its part, is a dedicated tactical department within the police force,*

²² See Annexure A to the Written Submissions.

subordinated to the Ministry of Home Affairs, with extensive prerogatives to apply force in combating terrorism (see section 1(2) subsection 15 of the Police Act quoted in paragraph 16 above). **For the Court, this supervision, eminently political** (as observed by the Constitutional Court, see point 105 of the decision quoted in paragraph 20 above) but carried out by the Minister of Justice who appears to be formally independent of both the TEK and of the Minister of Home Affairs – **is inherently incapable of ensuring the requisite assessment of strict necessity with regard to the aims and the means at stake.** In particular, although the security services are required, in their applications to the Minister for warrants, to outline the necessity as such of secret information gathering, this procedure does not guarantee that an assessment of strict necessity is carried out, notably in terms of the range of persons and the premises concerned (see section 57 (2) of the National Security Act quoted in paragraph 17 above).

77. As regards the authority competent to authorise the surveillance, authorising of telephone tapping by a non-judicial authority may be compatible with the Convention (see, for example, *Klass and Others*, cited above, § 51; *Weber and Saravia*, cited above, § 115; and *Kennedy*, cited above, § 31), provided that that authority is sufficiently independent from the executive (see *Roman Zakharov*, cited above, § 258). However, **the political nature of the authorisation and supervision increases the risk of abusive measures.** The Court recalls that the rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge...
78. The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures.
82. The Court notes at this juncture the liability of the executive to give account, in general terms rather than concerning any individual cases, of such operations to a parliamentary committee. However, it cannot identify any provisions in Hungarian legislation permitting a remedy granted by this procedure during the application of measures of secret surveillance to those who are subjected to secret surveillance but, by necessity, are kept unaware thereof. The Minister is under an obligation to present a general report, at least twice a year, to the responsible parliamentary committee about the functioning of national security services, which report, however, does not seem to be available to the public and by this appears to fall short of securing adequate safeguards in terms of public scrutiny (see *Roman Zakharov*, cited above, § 283).
47. In this context, it is apposite to evaluate the provisions of the Act and Regulations issued thereunder:
 - a. The Act contains no provision whatsoever to govern omission or deactivation of the Aadhaar number. Insofar as the Act permits the same to be determined by the UIDAI in terms of S. 23(2) read with Section 54(2)(l), without providing any guiding norm for the same, there is excessive delegation of power. Consequently, the Act is liable to be struck down inasmuch as it fails to lay down the circumstances in which a person can be deprived of her Aadhaar number;

- b. At any rate, the procedure for omission and deactivation of Aadhaar numbers is violative of the principles of natural justice, as it does not contemplate any hearing being offered to the concerned person. There is also no judicial oversight over this process;
 - c. Equally, the Act contains no provisions for redressal of grievances in the event of omission or deactivation of Aadhaar numbers.
 - d. Grievance redressal mechanism, through a contact centre established in terms of Regulations 30(2) read with Regulation 32 is grossly insufficient and illusory, inasmuch as it contains no defined procedure for such grievance redressal whatsoever, much less any judicial supervision.
 - e. While S. 34 to 41 provide for offences under the Act, it is not open to the affected party to approach the Courts for redressal, since, unless the complaint is made by or under the express authorization of UIDAI, no cognizance would be taken.
 - f. That apart, there is no cogent procedure or mechanism by which the offence can be investigated or such person can be arrested and prosecuted. This makes any breach of data protection and privacy norms almost impossible to address, investigate and prosecute.
 - g. Similarly, S. 33(2) which permits disclosure of identity information and authentication records under directions of an officer not below the rank of Jt. Secretary to the Central Government in the interests of national security, contains no provision to permit judicial review.
 - h. The composition of the Oversight Committee (which reviews such order) evidences that the same comprises only of bureaucrats). Given that an order under S. 33(2) (which can remain in effect for three months and thereafter can be further extended) empowers real-time surveillance, absence of a judicial member in the Oversight Committee renders the same completely unconstitutional.
48. Thus, the Aadhaar Project is therefore bad for the absence of effective judicial oversight.

VII. THE AADHAR PROJECT HAS A CHILLING EFFECT ON THE EXERCISE OF FUNDAMENTAL RIGHTS

- 49. As borne out from the above, the Act and other laws/ rules/ circulars, which make Aadhaar linking mandatory, enable mass collection and retention of data of all persons without any limitation as to purpose, leading to mass surveillance and profiling.
- 50. Upholding the validity of the Aadhaar Project would not only sound a completely discordant note with decisions taken and development of law by Courts abroad, but also constitute a giant leap backward for fundamental and human rights in this country.
- 51. The right to freedom includes the right to be free of unwarranted profiling and surveillance because the same has a chilling effect on personal liberty and on other freedoms as contained in Part III of the Constitution.
- 52. The well-known impact of surveillance on the human mind and freedom was recognised in the landmark dissenting judgment of HMJ Subba Rao in *Kharak Singh v. State of UP*, (1964) 1 SCR 332 when it was held at p. 360

191
Annexure R-6

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.....	3
(A)	Unauthorised and Excessive Data Collection – <i>Illegal Collection of Personal Data</i>	4
(B)	State Resident Data Hubs – Illegal Sharing of Aadhaar Data	6
(C)	Aggregation of Data within the CIDR – Illegal Storage of Data	10
(D)	Access to the CIDR is in contravention of the Aadhaar Act – Illegal Access of Data	13
(E)	Remote Seeding Facility of Aadhaar – Illegal Sharing and Usage of Aadhaar Data	15
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.....	18
(A)	Lack of Administrative Due Diligence prior to introduction:	18
(B)	Failure of Aadhaar.....	28
(C)	Resulting Failure Rates and Aadhaar Exclusions:	29
III.	Absolute Lack of Security in the Aadhaar Project amounts to a gross violation of the Right to Privacy under Article 21	33
(A)	Contracts with Foreign Agencies render the Aadhaar 'insecure ab initio'	33
(B)	Failure to ensure Security of Private Data.....	41
IV.	Consequences of Aadhaar data being used for other purposes, such as surveillance and administration	53
(A)	Purpose Specification and Use Limitation	53

192

(B)	European Union Jurisprudence on Data Collection, Retention and Usage	54
(C)	State Surveillance	58
(D)	Algorithmic Governance and Aadhaar Data	59
V.	Challenges to the Aadhaar Act and Regulations thereunder	63
(A)	Excessive Delegation of Powers by the Aadhaar Act to the UIDAI	63
(B)	That Section 33(2) of the Aadhaar Act is Overbroad and Constitutionally Invalid	68
(C)	That Section 57 of the Aadhaar Act is Overbroad and Constitutionally Invalid	74
VI.	The Aadhaar Act renders the Orders of this Hon'ble Court ineffective	76
VII.	Conclusion	80

193

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 as **Annexure-6** at paragraph 1.1, running page 28 and paragraph 2.2.1, running page 29.

199

B

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*

195

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 disbursement 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

196

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.

197

(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.

198

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 as 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.*

199

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

200

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.

- 201
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.

202

(F) 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

203

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;

204

(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.

Annexure R-7

IN THE SUPREME COURT OF INDIA

205

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

ADDITIONAL AFFIDAVIT DATED 09.03.2018 ON BEHALF OF

RESPONDENT NO. 3

I, Rajendra Prasad Pant, son of Late Sh. C. B. Pant aged about 54 years, occupation Assistant Director General of Unique Identification Authority of India, with office at UIDAI Headquarters, Jeevan Bharati Building, New Delhi, do hereby solemnly affirm and say as follows:

1. That I am working as the Assistant Director General of Unique Identification Authority of India, the Respondent No. 3 in the present Writ Petition. I am conversant with the facts and circumstances of the present case and I am duly authorized by respondent No. 3 to affirm this affidavit on behalf of the respondent in the present Writ Petition and as such I am competent to swear the present Affidavit.
2. That during the arguments of the Petitioner, several affidavits have been relied upon including those filed in January, 2018 and an additional affidavit filed by the Petitioner in W.P. (C) 829 of 2013

206

on 16.02.2018 during the on-going hearings. Many of the averments relate to facts which have not been raised earlier and therefore it has become necessary to controvert those averments.

3. That in order to assist this Hon'ble Court to appreciate the facts in its totality, the present affidavit is being filed by the answering respondent refuting some of the allegations made during the hearings by the Petitioners.

4. The present Affidavit can be broadly categorized under the following broad heads:-

I. Allegations dealing with Exclusion

II. Allegations dealing with Data Security

III. Allegations dealing with Privacy & Surveillance

IV. Allegations dealing with Inaccurate Claims qua Savings

5. The Answering Respondent denies each and every allegation made by the Petitioners during oral hearings except those which are specifically admitted hereinafter.

I. ALLEGATIONS DEALING WITH EXCLUSION

6. The allegations relating to exclusion have already been dealt with by the answering respondent in earlier Common Additional Affidavit dated 15.01.2018 filed by it at Paras 186 to 189 at Pages

207

156 to 158. Additionally, it is submitted that any exclusion of genuine beneficiary contrary to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter referred to as the "Aadhaar Act") is, at best, a breach of the extant legal regime or a misuse/abuse of the law and cannot be the touchstone to assess the constitutional validity of the Act. In fact, Regulation 32 in Chapter VII of the Aadhaar (Enrolment and Update) Regulations, 2016 has a grievance redressal mechanism under which grievances can be registered for any unlawful exclusion of beneficiaries due to failure of authentication or such other reason related to the answering respondent. The grievance redressal mechanism under the respective laws may also be availed of depending on the nature of grievance. Moreover, the remedy under Article 226 of the Constitution is also available for violation of statutory rights under the Aadhaar Act and other legislations, wherever applicable like the National Food Security Act but that cannot be a ground to challenge the provisions of the Aadhaar Act itself. To put it simply, non-compliance with or breach of the provisions of the Aadhaar Act can never be a ground to strike down the Act itself.

7. Having said that, it would be appropriate to individually deal with allegations and instances of alleged exclusion on account of Aadhaar raised by the Petitioners.

208

Aadhaar is based on inclusion and not exclusion as wrongly alleged by the Petitioners

8. The Petitioners argued that Aadhaar has been an instrument of exclusion. The Petitioners claim that 99.9% of persons who have an Aadhaar obtained it on the basis of pre-existing IDs as per an RTI reply by the authority and that only 0.03% used the introducer system and it is therefore alleged that there was no genuine need for Aadhaar and that Aadhaar acts as a tool of exclusion. It is submitted that Aadhaar enrollment is possible on the basis of any of the large number of identity documents including undertaking given by a Head of Household, parent or guardian, certificate from anganwadis, schools, a certificate from a village panchayat head or a tehsildar or a rent agreement amongst others. These identity documents, though acceptable for Aadhaar enrolments, would not be acceptable for all purposes to establish identity. For example, a person with a certificate from a head of the household, or a village panchayat head, or a school teacher or ananganwadi sevikas may not be able to access his rations or open a bank account even though it is an acceptable underlying identity document for Aadhaar enrolment and he will be able to use it as a proof of identity for generation of Aadhaar number. Local IDs are often either informal in nature or in local vernacular language which usually does not work in other States. Migrant workers usually face this problem who move from State to State in search of employment and have no credible ID which would be acceptable through out the country for variety of services. This phenomenon was referred to as the 'poverty premium' wherein the poor had to pay a premium to prove their identity

209

whenever they needed to access a service. Existing identity documents were also often found to be circular wherein if you required a ration card, you would have to provide your electricity bill and vice versa. Therefore, for obtaining Aadhaar, a much wider list of underlying identity documents were made acceptable so as to enable the access of an Indian resident to a universal and credible identity document, which is nationally portable and verifiable. The reason behind UIDAI accepting such identity documents was inclusiveness so that no genuine person is left out from State's benefits, services or subsidies for want of an Aadhaar number. In fact, the existential being of an individual has been recognized by Aadhaar and given the dignity that it deserves. Therefore, once he obtains an Aadhaar number he can apply for for a host of benefits and subsidies which he would have otherwise not been accessible on account of lack of a robust universally acceptable identity document. Hence, the rationale of the Petitioners that merely because 0.03% people used the introducer system, the rest of the country already had a pre-existing identity document is simplistic, misleading and fails to encompass the complexity of the ground realities, and hence liable to be rejected. The fact that Aadhaar has given the people of India a credible identity document, large numbers of whom did not have any proper identity document need not be looked further than the fact that today Aadhaar is the most widely held identity document by 120.32 Crore residents of India. This figure is more than twice the number of Voter I-Cards

210

or EPIC Cards which stands at approximately 60 Crores and is the next most widely held identity document in the country.

9. Therefore, Aadhaar number being the most widely held form of identity document with the widest coverage amongst the people of India the possibility of exclusion on account of not having Aadhaar is far less than not having any other identity proof. Rather, given that the Aadhaar number/ card is the most widely held identity document, the present petitioner's prayers would cause serious hardship to such residents, for many of whom it is the only credible identity proof that they possess or those like the old and infirm, migrant workers etc. who are dependent on the conveniences which Aadhaar provides like direct benefit transfers etc.

[True copy of the Proof of Identity documents accepted for Aadhaar enrolment is attached as Annexure R-1 at Pg. 107 to 109]

10. It is submitted that Section 7 of the Aadhaar Act states that the 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 the Consolidated fund of India require that such individual undergo authentication or furnish proof of possession of Aadhaar number. Therefore, if a person is unable to undergo authentication for whatever reason, the Act itself clearly provides that it would suffice to furnish proof of possession of Aadhaar number for receipt of subsidy, service or benefit. Section 8 (3) (c) of the Aadhaar Act is meant for a situation, if and

211

when, for any reason authentication fails, then the requesting entity will be required to provide alternatives to submission of identity information. Therefore, the argument of the Petitioner that authentication errors lead to exclusion and denial of an entitlement or benefit is completely misplaced and premised on an incorrect reading of the law since an individual who has been unable to undergo authentication for any reason may be able to obtain his entitlements by furnishing proof of possession of Aadhaar number, the veracity of which can be verified by the authorities concerned through prescribed means. Therefore, if there are any denials contrary to the Aadhaar Act, then the remedy is to approach the concerned Department or lodge a grievance before the Centre for Grievance Redressal under Regulation 32(supra) and departmental action on the basis of complaint by the beneficiaries should be initiated against errant officials. The Aadhaar Act has been enacted with an object to provide for, as a good governance, efficient, transparent and targeted delivery of subsidies, benefits and services to genuine beneficiaries. Therefore any exclusion of genuine beneficiaries who hold an Aadhaar number will be strictly dealt with in accordance with law. It is, however, reiterated that a breach of the provisions of the Act can never be a ground to question the Act itself.

11. Moreover, the Answering Respondents' own understanding of the Aadhaar Act is also inclusive in nature and places necessary safeguards to prevent exclusion of any genuine beneficiaries.

212

Notifications under Section 7 of the Aadhaar Act 2016 provide that if people are not able to enroll for Aadhaar due to lack of enrolment facilities in the nearby areas, then they can register their request for Aadhaar enrolment before the appropriate authorities giving their contact details so that as and when enrolment facilities are set up in the area, such persons can be enrolled for Aadhaar and till such time benefits will continue to be given even if they have not enrolled for Aadhaar before deadline.

12. To ensure inclusiveness in PDS distribution, the UIDAI in its Circular dated 24.10.2017 has also laid down the exception handling mechanism to prevent exclusion of genuine beneficiaries if and when for any reason their biometric authentication fails. The exception handling mechanism laid out in the Circular is to the following effect:-

"That Circular No. 23011/Gen/2014/Legal-UIDAI dated 24th October, 2017 issued by the Unique Identification Authority of India.(UIDAI) was issued with regards to Exception handling in Public Distribution Services and other welfare schemes. The relevant extracts from the circular are quoted as follows:

"3. It has come to notice that some beneficiaries are being denied the benefit, subsidy or service for various reasons such as not having Aadhaar, failure of authentication; and other extraneous circumstances like electricity outage, internet connectivity issues etc. despite above provisions of Aadhaar Act and other adequate mechanisms to handle such exemptions already provided in the Regulations and notifications issued under Section 7.

213

4. Therefore, the following exception handling mechanisms and back-up identity authentication mechanisms may be followed for implementation to ensure seamless delivery of subsidy, benefit or service to beneficiary:

a. Till the time Aadhaar is assigned to a beneficiary, he/she shall be provided subsidy, benefit or service based on alternate identification document as notified by the ministry/Department in the relevant notification issued under the provisions of Section 7 of the Aadhaar Act, 2016. The notifications also give powers to both Central Ministry and State Government (as the case may be) to add more alternate documents depending on local conditions.

b. In case of failure of Biometric authentication due to network/connectivity issue or due to poor biometric of resident etc, he/she shall be provided subsidy, benefit or service based on possession of Aadhaar by him/her as provided in Section 7 of the Aadhaar Act, 2016 and notifications.

c. In case of family based scheme, such as PDS, an option shall be provided that any member of the family can authenticate and receive the benefit, as notified by the Ministry/Department in the relevant notification issued under the provision of Section 7 of the Aadhaar Act, 2016. This flexibility should be used for ensuring delivery of benefit in case biometric authentication for a member (senior) fails.

d. The State Government/Implementing agency should also make special arrangements for bed ridden senior residents to get them verified/authenticated including but not limited to sending a village level worker to their home for this purpose.

e. All such exception handling shall be recorded in the system and steps be taken to avoid any misuse of the exception. The front end services provider shall also maintain record of exception such as

214

beneficiary and other supporting document as notified by the Ministry/Department.

f. The Ministry/Department shall devise and implement mechanism for audit and inspection of such exceptions. ”

[A Copy of the Circular dated 24.10.2017 is marked and attached as

Annexure R-2 at Pg. 110 to 111]

13. The Aadhaar Act, 2016 is very clear that those who do not have Aadhaar will be required to apply for Aadhaar and till the Aadhaar number is assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or services. The answering respondents have always maintained that the intention is to ensure that no one is denied any subsidies or benefits for lack of Aadhaar until the Aadhaar number is assigned, or on the grounds of lack of linking, or technical difficulty in biometric authentication.

14. To the same effect are the instructions and circulars issued by Cabinet Secretariat and Ministry of Consumer Affairs, Food and Public Distribution.

[True Copy of the DBT Mission, Cabinet Secretariat OM dated 19th December 2017 on Exception Handling in Use of Aadhaar in Benefit Schemes of Government is marked and attached as Annexure R-3 at Pg. 112 to 113]

[True Copy of Letter dated 24th October, 2017 by Ministry of Consumer Affairs, Food and Public Distribution to States/UTs on

215

Aadhaar seeding with ration cards is marked as Annexure R – 4 at Pg. 114 to 115].

15. The inclusiveness brought about by Aadhaar can be seen from the following instances.
16. Aiyar, S. in his book, Aadhaar – A Biometric History of India's 12 Digit Revolution discusses a true story about Nathu Ram, a villager from Madhya Pradesh and how Aadhaar helped someone like him:

"It was a narration of the hardships Ram went through to collect his MGNREGS dues. He had to walk 6 km to the nearest bus stop. There he had to wait for a bus, which wasn't regular, would arrive over-crowded and might also break down on the way. Then he had to have the money to buy a ticket to find a toehold on that bus and travel 14 km to the nearest bank branch. He then had to wait nearly two hours, in the hope that his turn would come before the bank closed for the day. If he was lucky, he would get his money the same day. If not, he would have to camp on the road outside, until the branch opened on the next working day. Having finally got his dues for the month, Ram would travel back home, 14 km by bus and 6 km by foot. Given the uncertainty of getting his dues from the bank, Ram would have already borrowed from the local money lender at usurious rates. Only after he had repaid that bridge-loan, or a part of it, if he had any money left, would he be able to get to the local fair-price ration shop to buy his family's grains and cooking fuel."

216

17. The Mahatma Gandhi National Rural Employment Guarantee Scheme pursuant to the MGNREG Act, 2005 assures livelihood security to the rural poor by guaranteeing a minimum of 100 days of wage employment annually to every household whose adult members volunteer to do manual unskilled work. There are 11.2 crore active workers registered in the MGNREGS. Of these, 9.9 crore have their job cards linked with their Aadhaar number. More than 28.47 crore Aadhaar based payment transactions transferring wages over Rs.27,117 crore have been already done. Those who are entitled to receive MGNREGS wages and have Aadhaar-linked bank accounts can authenticate their identity at their doorstep/ neighbourhood. This ensures that amounts are credited to their bank accounts immediately, allowing them to withdraw money with ease thereby furthering the end of financial inclusion. This saves them the trouble of going to the nearest bank, often at distances in excess of 40 km, thereby saving loss of a day's wages. MGNREGS workers are withdrawing their wages using Aadhaar bio-metric authentication every month at their doorstep / neighbourhood without middlemen and any delay. Aadhaar ensures that workers no longer have to undertake back-breaking travel and loss of wages to go to their bank branches to receive their daily wage. Therefore, it is the right to livelihood of millions of Indians, which is facilitated by Aadhaar.
18. Likewise, those who are entitled to receive such pensions under the National Social Assistance Programme (Old Age Pensions, Widow

217

Pensions, Disability Pensions) and have Aadhaar-linked bank accounts can authenticate their identity at their doorstep/ neighbourhood. This saves old-age pensioners, widows and the disabled the trouble of going to their bank branch to receive their pensions which is onerous particularly in far-flung rural areas.

19. Similarly, at present, all pensioners, including ex-servicemen have to visit the bank branch where their pension account has been opened annually to demonstrate that he/ she is alive and therefore entitled to receive pension. This is an onerous affair as this proof cannot be given anywhere in India and requires senior citizens to travel to the particular branches where their pension accounts exist, to continue to receive pensions, irrespective of where they reside at present. The Jeevan Pramaan scheme dispenses with this requirement of personal appearance. Using Aadhaar, the pensioner can go to any bank/common service centre in India which has the Jeevan Praman facility. This is widely available across India. At such centres, he/ she can use Aadhaar to authenticate that he/she is alive, saving the old pensioners the burden of travelling to their original bank branches to receive their pension. As on today, 1.68 crore pensioners are using their Aadhaar linked accounts to receive pensions.
20. All of the above are examples of a thriving and inclusive system which is possible on account of Aadhaar.

218

Allegations of starvation deaths on account of Aadhaar

21. That the contents of the Affidavits of Ms. Reetika Khara and Siraj Dutta dated 06.01.2018 filed in I.A. No. 6901/2018 in W.P. (C) No. 797/2016 dealing with the death of one Premani Kunwar of Korta village, Danda Gram Panchayat, Danda block, Garhwa, Jharkhand is vehemently denied as incorrect and based on misinformation. This relates to a report of fact finding into the death of Premani Kunwar of Korta village, Danda Gram Panchayat, Danda block, Garhwa, Jharkhand allegedly due to starvation, as she was denied her ration from the local PDS shop, for not possessing Aadhaar. Pursuant to the media report, a team of officers from the UIDAI Regional Office at Ranchi visited the spot to ascertain the details. Parallel to this, an enquiry was also conducted by the local Block Development Officer (BDO) and by the local police. Two criminal cases have been registered related to the instant case. Field Enquiry has revealed the following:-

- (i) Smt. Premni Kunwar w/o Late Mutur Mahto was a 64 year old widow living with her thirteen year old son Uttam.
- (ii) Late Mutur Mahto's first wife Shanti Devi died 25 years back and she left behind four sons and two daughters, of whom Sunil Mahto is unmarried.
- (iii) Premni Kunwar's widow pension was being deposited in her postal account no.XXX0308. She also had a bank account no.XXXX5240 in Danda Branch of SBI.

219

- (iv) On 8.9.2017, Rs.1200/- was withdrawn by Premni Kunwar from the said account. Her Aadhaar no. xxxxxxxx7606 was found to be linked with her aforesaid SBI Bank account.
- (v) Another bank account bearing no. XXXXX7614 in the name of Late Shanti Devi was also found to be linked with the same Aadhaar number i.e., xxxxxxxx7606 (on 10.10.2017). Enquiry revealed that Smt. Premni Kunwar was first enrolled using her own name in 2013, but in 2015, she updated her name to Shanti Devi.
- (vi) The seeding of bank account no. XXXX7614 of Shanti Devi with Aadhaar number (fraudulently updated by Premani Kunwar as Shanti Devi in 2015) wherein Rs.829 per month of widow pension was being received on the basis of digital life certificate of Shanti Devi.
- (vii) In both the said SBI accounts, i.e., at Danda and at Garhwa (Piprakalan Branch) the photo of Premni Kunwar was seen in the records.
- (viii) It is pertinent to note therefore, that Premni Kunwar was operating two pension bank accounts in two different names – i.e. one in her real name and another in the name of Shanti Devi, who was since long deceased. In the latter account Premni Kunwar was fraudulently posing as Shanti Devi and operating the latter's bank account for years after the death of Shanti Devi and was withdrawing the pension meant for Shanti Devi. Only after Aadhaar

220

was required for verification of bank accounts, she had no option but to authenticate her Aadhaar identity and when she authenticated her Aadhaar identity as Shanti Devi, her other pension account which she was operating as Premni Kunwar stopped receiving credits for pension. This is precisely the kind of fraud where a person has multiple bank accounts under different names can get exposed through Aadhaar authentication as evident from this case. This, inter alia, is the reason behind making Aadhaar mandatory for bank accounts.

- (ix) Thereafter, on 6.11.2017, an amount of Rs.30,000/- was withdrawn from the account of Shanti Devi by Premni Kunwar. The mobile no. in the withdrawal slip reflected the number of Sunil Mahto (step-son of deceased). The district authorities and the Medical Report have categorically ruled out the possibility of starvation.
- (x) The postmortem report revealed semi digested food in the stomach coupled with the fact that Rs.30,000/- was withdrawn in month of November, 2017 it cannot be said that Premani Kunwar died of starvation. It appears from the preliminary enquiry report into the death of Smt. Premani Kumar, conducted by Superintendent of Police, Garhwa, Jharkhad that Sunil Mahto is the accused conspirator of fraudulent activities. Sunil Mehto was there in CCTV footage when the money was withdrawn from bank on 06/11/2017.

221

(xi) The local S.P. has informed that the lady Premani Kunwar was sick and she died at the age of 64 due to failing health. However, the deceased lady Premani Kunwar and her step son Sunil Mahto as per S.P.'s report prima facie appear to be involved in fraudulent activities and impersonation, which are offences both under the I.P.C. as well as the Aadhaar Act. The fraudulent act by way of Aadhaar updation by Premani Kunwar in the name of Shanti Devi amounts to impersonation and is a punishable offence under Section 35 of the Aadhaar Act, 2016.

22. It is denied that the 11 year old Santoshi Kumar died due to lack of Aadhaar. This is evident from the fact that the entire family had Aadhaar numbers since 2013. It is submitted that the concerned Government could not have denied rations under the law to Santoshi Kumar even assuming that her ration card was not Aadhaar linked. The extant notifications require the Government to give alternatives if, for some reason, authentication is not possible and even furnishing proof of possession of Aadhaar number would suffice under the exception handling mechanism discussed above. Therefore, the violation of the law by certain State Government officials cannot be used as a ground to discredit Aadhaar or call into question the validity of the law itself.
23. All field agencies should be extremely sensitive in ensuring that the benefits, subsidies or programmes flow to the genuine

222

beneficiaries. The field agencies should be sensitive to the needs of the people and ensure their actions do not result in denial of benefits to genuine beneficiaries. To ensure seamless delivery of subsidy, benefit or service to the eligible beneficiaries of the various schemes, UIDAI has also issued a circular dated 24.10.2017 (*supra*) to all Ministries and State Governments on Exception Handling in PDS and other welfare schemes.

[True Copy of the Redacted Aadhaar cards of Santoshi Kumar and her family members are attached as Annexure R-5 at Pg. 116 to 117]

24. It has been stated in the Affidavit of Siraj Dutta that one Etwariya Devi in Sonpurwa Village in Jharkhand, had passed away on 25th December, 2017. It was alleged and argued by the Petitioners that the death of Etwariya Devi was on account of starvation caused by exclusion on account of Aadhaar. The allegations with respect to Etwariya Devi's death in the Affidavit relied upon by the Petitioners is denied and the facts are being placed in its correct perspective based on the preliminary report submitted by the Regional Office of UIDAI. The Preliminary report states that a resident by the name of Etwariya Devi expired on 25th December, 2017. The Regional Office Ranchi has investigated the matter and met with the family members of the deceased and the concerned district officials. The District Authority has also investigated into the matter by a three member committee comprising of Block Development Officer (BDO), Majhigaon; Supply Officer cum

223

BDO, Bardiha and Director, Social Security, Garhwa. They have also taken the statement of her son. The findings of the Committee are as follows –

- I. During the Course of investigation the family members and neighbours intimated that she died a natural death.
- II. Her daughter in law intimated that food was prepared by the family but could not be consumed due to her sudden demise. The same has been confirmed by her son also.
- III. No post-mortem has been done in this case.
- IV. As per the statement given by her own son, Etwariya Devi died a natural death and not caused by cold, lack of money or lack of food.
- V. She was a beneficiary of Pension under National Social Assistance Programme (NSAP) and she was receiving regular pension in her account from the district. This is evident from the fact that her account has been credited with Rs. 1200 on 08.09.2017, Rs. 1200 on 24.10.2017 and Rs. 600 on 07.12.2017. Her bank account was showing Rs. 1233/- as balance amount.
- VI. It was also found that the family is getting ration regularly from the Local PDS shop. The family has received ration on 5th October, 2017 even though Aadhaar authentication was not successful but ration was given by taking note on the register. Likewise on 27th December, 2017 ration was taken by her Daughter

224

in law upon successful Aadhaar authentication for both months of November and December, 2017 together.

25. From an analysis of the above factual scenario, it appears that Etwariya Devi's death was completely unrelated to Aadhaar and was due to natural consequences as stated by her own family members. Therefore, the allegations made against Aadhaar are baseless and unsubstantiated.

No exclusion of leprosy patients under Aadhaar who are covered by the biometric exception regulations

26. It is submitted that Aadhaar was conceived to provide a universal and credible identity document to all eligible residents of India. Aadhaar, being inclusive in nature and sensitive to the fact that a large number of people like leprosy patients would not have proper biometrics, suitable exceptions were also contemplated under the Aadhaar regime. So far, 1.14 Lakh people have been given complete biometric exception and over 1.8 Crore people have been enrolled with some biometric exception or the other. Complete Biometric exception means that neither the Iris nor the Ten fingerprints were available for enrollment. In this regard, Regulation 6 of the Aadhaar (Enrollment and Update) Regulations, 2016 can be referred to –

“6. Enrolment of residents with biometric exceptions.

- (1) For residents who are unable to provide fingerprints, owing to reasons such as injury, deformities, amputation of the fingers/ hands or any

225

other relevant reason, only Iris scans of such residents will be collected.

(2) For residents who are unable to provide any biometric information contemplated by these regulations, the Authority shall provide for handling of such exceptions in the enrolment and update software, and such enrolment shall be carried out as per the procedure as may be specified by the Authority for this purpose."

27. Similarly, if there are any authentication failures due to unavailability of biometrics, suitable exception handling mechanism has been laid down for all schemes by various circulars discussed above. Therefore, the petitioner's contention that leprosy patients would be excluded from the benefits of Aadhaar is misplaced and based on an ignorance of the law.

Rejection of 6.23 Crore Aadhaar enrolments as duplicates

28. The figure provided in RTI Reply with Ref No. F-12013/1223-1229/2016-RTI-UIDAI dated 04.01.2017 stating that 6.23 Crore enrolments have been rejected as biometric duplicates by the UIDAI does 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 virtually impossible

226

for all these features 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 these individuals have already registered in the system it rejects the enrolment application. It used to also happen that multiple people would put their biometric details like fingerprints for Aadhaar generation either as a fraudulent exercise or by mistake, which 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 to 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. In fact, upon further enquiry by the answering respondent it was found that around 9.05 crore enrolment were rejected as genuine duplicates since they all already had Aadhaars

against their earlier enrollments. Notwithstanding the 6.23 crore duplicates, as of today there are more than 1.2 billion enrollments. This is coupled with the fact 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.

29. The Aadhaar system has a mechanism to ensure that individuals whose enrolment application has been rejected for non-availability of both fingerprint and Iris biometrics (such as in the case of disability) still have a way to enrol. This type of enrolment follows biometric exception process wherein the enrolment operator marks application as biometric exceptions during the Aadhaar enrolment. Another vulnerable population is people who do not have supporting documents such as the proof-of-identity and/or proof-of-address. For such cases Aadhaar has implemented an Introducer system wherein a UID/Registrar appointed Introducer will vouch for the applicants' data forming a valid application. Thus, the UIDAI ensures that, under no circumstances will any eligible resident shall be denied an Aadhaar number even if they do not have requisite documents or there is a lack of availability of personal biometrics for reasons of disability.

228

46. Whether Aadhaar is required for Indians living abroad?

There are retired officers who reside outside India. Such persons who live abroad are neither required to get Aadhaar nor have their bank accounts etc verified by Aadhaar. The Aadhaar Act 2016 defines "resident" to mean an individual who has resided in India for a period or periods amounting in all to 182 days or more in the 12 months immediately preceding the date of application for enrolment. Section 3 entitles only such residents of India to obtain an Aadhaar number. Therefore, for non-residents, neither is there any requirement to get Aadhaar nor is there a requirement to have their bank accounts, etc verified with Aadhaar. The above position has been clarified by the UIDAI Circular dated 15.11.2017. [True Copy of the UIDAI Circular dated 15.11.2017 is marked as Annexure R - 6 at Pg. 118 to 120]

47. Exclusion by private parties from essential services like hospital for want of Aadhaar

During the hearing, an incident was highlighted by the Petitioner's Counsels that a lady had to deliver a baby outside a Gurgaon based hospital since the hospital denied her entry allegedly for not possessing Aadhaar. No law has been made imposing any mandatory condition for treatment in hospitals. As such the Gurgaon based hospital, which allegedly denied entry to a lady who had to deliver a baby outside was clearly acting contrary to the

229

established legal position and the Constitutional entitlement of the lady under Article 21 for immediate medical attention.

II. ALLEGATIONS DEALING WITH DATA SECURITY

30. The allegations relating to data security have already been dealt with by the answering respondent in earlier Common Additional Affidavit dated 15.01.2018 filed by it at Paras 90 to 112 at Pages 77 to 90 read with Para 190 to 205 at Pages 158 to 165. Additionally, it is submitted that the Petitioner has relied upon several affidavits filed a few days before the commencement of the hearing, which requires to be traversed and controverted.

Reply to Affidavit dated 13.01.2018 by Rakesh Goyal filed on 16.01.2018 in W.P.(C) 342/2016

31. During the oral arguments by the Counsel for the Petitioners, a lot of emphasis was placed on the affidavit dated 13.01.2018 of one M. Rakesh Goyal filed on 16.01.2018 in W.P (C) 342 of 2017. The said Affidavit filed by Dr. Rakesh Goyal, Director and Principal Consultant of Sysman Computers (P) Limited has cited (a) inherent design faults in the Aadhaar project that severely compromise the safety and security of citizens' biometric data; and (b) that based on the audits done by the petitioner for various AUAs, biometrics captured during the Aadhaar authentication process are being stored by entities other than UIDAI / CIDR. The contents of the said Affidavit are denied as incorrect, made in bad faith and with ulterior motives which will be demonstrated hereinafter.

230

32. Dr. Rakesh Goyal had summarised "Six methods of Hacking of Aadhaar Biometric Data". As stated by Dr. Rakesh Goyal these are based on the various audits done by Sysman Computers (P) Limited for the Authentication User Agencies (AUAs) of UIDAI. The deponent has clearly stated that he has no idea about the security of CIDR and related infrastructure and kept the same out of scope of the article and that this article is limited to the security of Biometric information collected by the AUAs from the residents as part of authenticating the residents for providing various services. The above assertions made by the deponent are denied. It is submitted that:-

- i. To strengthen the compliance by AUAs/KUAs to Aadhaar Act 2016 and its Regulations, UIDAI had issued a notice dated 28-Feb-2017 to all AUAs/KUAs to submit an Audit compliance report to UIDAI by 31-March-2017. UIDAI had also mandated the AUAs/KUAs to issue a compliance certificate against the points mentioned in the notice. (UIDAI requests submission of audit reports from AUAs by March end every year).
- ii. One of the requirements of the notice was for AUAs/KUAs to get their Authentication applications audited by STQC/CERT-IN certified information system auditor(s) and for AUAs/KUAs to submit the audit report to UIDAI.

231

- iii. As per the affidavit, Sysman Computers (P) Limited was engaged by 25 AUAs/KUAs for conducting audit of their Authentication applications.
- iv. Sysman Computers (P) Limited is CERT-In empaneled security auditor as per the CERT-In website since 2005.
- v. As per the records available with UIDAI, 15 of these audit reports were submitted to UIDAI in 2017 by the individual AUAs which were audited by Sysman Computers(P) Limited. The status of compliance reported by Sysman Computers (P) Limited for points related to storage of Biometric / PID block in 15 of the Audit reports submitted to UIDAI by the AUAs has been mentioned below:

Table 1 – Biometric/ PID storage related checklist points					
Biometric storage controls	PID block captured for Aadhaar authentication must be encrypted during capture and should never be sent in the clear over a network.	The encrypted PID block should not be stored unless it is for buffered authentication for a short period of time and after transmission, it should be deleted	Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database	PID block captured for Aadhaar authentication must be encrypted during capture and should never be sent in the clear over a network	The encrypted PID block should not be stored unless it is for buffered authentication for a short period of time and after transmission, it should be deleted. Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database
AUA org					

232

NSDL - PAAM	Compliant	Compliant	Compliant	Not Applicable	Not Applicable
NSDL - eNPS	Compliant	Compliant	Compliant	Not Applicable	Not Applicable
NSDL - Vastrakalyan	Compliant	Compliant	Compliant	Compliant	Compliant
NSDL - eSign	Not Applicable	Compliant	Compliant	Not Applicable	Not Applicable
Bharti AXA	Compliant	Compliant	Compliant	Not Applicable	Not Applicable
Equifax	Compliant	Compliant	Not Applicable	Not Applicable	Not Applicable
Future Generali	Compliant	Compliant	Compliant	Compliant	Compliant
HDFC Asset	Compliant	Compliant	Compliant	Not Applicable	Not Applicable
HDFC Ergo	Compliant	Compliant	Compliant	Not Applicable	Not Applicable
HDFC Housing	Compliant	Compliant	Compliant	Not Applicable	Not Applicable
ICICI Securities	Compliant	Compliant	Compliant	Compliant	Compliant
Jhaveri Securities	Compliant	Compliant	Compliant	Not Applicable	Not Applicable
Kotak Mahindra Bank	Compliant	Compliant	Compliant	Compliant	Compliant
Sharekhan	Compliant	Compliant	Compliant	Compliant	Compliant
UAE exchange	Compliant	Compliant	Compliant	Compliant	Compliant
Varachha Cooperative	Compliant	Compliant	Compliant	Compliant	Compliant
NDML	Compliant	Compliant	Compliant	Compliant	Compliant
SHCIL	Compliant	Compliant	Compliant	Not Applicable	Not Applicable

33. There is not a single non-compliance for the various Biometric related controls in the 15 audit reports available with UIDAI submitted by the Companies containing the audit certificates by Mr. Goyal.

34. It is inconceivable why Mr. Goyal would give a clean chit to the companies as a statutory auditor and then file before this Court an affidavit stating that these AUAs were capturing biometric information contrary to the law. The affidavit of Mr. Goyal appear to be motivated and lack any credibility and should outright be rejected.

35. Additionally, it is pertinent to note that Sysman Computers (P) Limited had attempted to participate in the Request for Empanelment (RFE) by UIDAI for "Empanelment of Certification

233

Agencies for certifying KUAs/AUAs/Sub-AUAs Authentication and e-KYC applications" dated 24/11/2017 and apparently did not meet the pre-qualification criteria to participate in the bid.

36. In their pre-bid queries Sysman Computers (P) Limited had requested to change the pre-qualification criteria of the RFE so that it could qualify in the UIDAI empanelment process and become one of the empaneled agencies. However, there were no changes made by UIDAI in the pre-qualification criteria to maintain the quality of agencies to be empaneled by UIDAI.
37. It is pertinent to note that the UIDAI vide Letters dated 17.01.2018, 24.01.2018 and 29.01.2018 has requested Mr. Rakesh Goyal for a list of all the Requesting Entities audited by his company, M/s Sysman Computers Pvt. Ltd. and also indicate the ones which had violated the provisions of Aadhaar Act, 2016 and the Regulations therein.
- [True copy of the letters dated 17.01.2018, 24.01.2018 and 29.01.2018 are marked and annexed as Annexure R - 7 (Colly.) at Pg. 121 to 123]
- [A reply was received on 29.01.2018 stating that the information sought by the UIDAI is not possible to be provided as he was bound by Confidentiality and Non-disclosure Agreements and Professional Ethics. True Copy of the letter date 29.01.2018 are marked as Annexure R-8 at Pg. to 124.]

234

38. It is evident that Dr. Rakesh Goyal, while on one hand, has given a compliance certificate to the companies that he has audited and on the other hand he has deposed before this Hon'ble Court on affidavit that during Audit of the AUAs/KUAs, many of the AUAs did not comply with the AUA Audit Compliance Checklist and when UIDAI asked him to disclose the list of companies he audited and those who were violating the Aadhaar Act 2016, he refused to provide the same citing confidentiality and non-disclosure agreement. He has also alleged that in some cases the entities being audited were storing biometric data. However, no such discrepancy has been brought out by him in his Audit certificates. Therefore, Dr. Rakesh Goyal has either acted in dereliction of his duty as an Auditor and has given an incorrect compliance certificate reports, or, if that is not true then he has made a false affidavit before this Hon'ble Court, because both his contradictory versions cannot stand together.

[A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for Bharti Axa Life Insurance Co. Limited dated 15.05.2017 is attached herein and marked as Annexure R-9 at Pg. 125 to 134]

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for Equifax Credit Information Services Private Limited dated 24.03.2017 is attached herein and marked as Annexure R-10 at Pg. 135 to 144.

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for M/S Future Generali India Life Insurance Company Limited

235

dated 25.03.2017 is attached herein and marked as Annexure R-11 at Pg. 145 to 154.

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for HDFC Asset Management Company Ltd. dated 28.03.2017 is attached herein and marked as Annexure R-12 at Pg. 155 to 163.

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for HDFC Ergo General Insurance Ltd. dated 24.03.2017 is attached herein and marked as Annexure R-13 at Pg. 164 to 172.

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for Housing Development Finance Corporation Ltd. dated 28.03.2017 is attached herein and marked as Annexure R-14 at Pg. 173 to 181.

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for ICICI Securities limited dated 04.04.2017 is attached herein and marked as Annexure R-15 at Pg. 182 to 191.

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for Jhaveri Securities Limited dated 29.03.2017 is attached herein and marked as Annexure R-16 at Pg. 192 to 200.

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for Kotak Mahindra Bank Limited dated 29.03.2017 is attached herein and marked as Annexure R-17 at Pg. 201 to 209.

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for NSDL Database Management Limited dated 29.03.2017 is attached herein and marked as Annexure R-18 at Pg. 210 to 219.

236

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for NSDL e-Gov Infrastructure Limited dated 28.03.2017 is attached herein and marked as **Annexure R-19 at Pg. 220 to 257.**

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for Sharekhan Limited dated 14.03.2017 is attached herein and marked as **Annexure R-20 at Pg. 258 to 267.**

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for Stock Holding Corporation of India Limited dated 27.03.2017 is attached herein and marked as **Annexure R-21 at Pg. 268 to 276 .**

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for UAE Exchange and Financial Services Limited dated 29.03.2017 is attached herein and marked as **Annexure R-22 at Pg. 277 to 285.**

A True Copy of the Compliance Audit Report by Dr. Rakesh Goyal for The Varachha Co-operative Bank Limited dated 29.03.2017 is attached herein and marked as **Annexure R-23 at Pg. 286 to 293]**

39. In the above mentioned affidavit, Dr. Rakesh Goyal, has also relied upon his own article dated 11th January, 2018 - "Six Methods of Hacking of Aadhaar Biometric Data". The affidavit also mentions that he had no idea about the security of CIDR and related infrastructure and kept the same out of scope of the article.
40. In response to the above affidavit, it is pertinent to re-iterate the various security measures in place to prevent unauthorized use of biometric data:-

237

a) Overall security measures taken by UIDAI for security of Biometric data collected by AUAs from the residents

UIDAI has taken several legal, governance and technical measures to ensure that the biometric data collected by the AUAs is secure.

These measures have been mentioned in 2 parts:

- Implementation of Registered devices as a technology measure to rule out any possibility of use of stored biometric and replay of biometrics captured from other source.
- Measures taken prior to implementation of Registered devices

i. Implementation of Registered devices

About Registered devices: 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 with time stamps etc. The device provider RD Service encrypts PID block before returning to the host application. This RD Service encapsulates the biometric capture, after signing and encryption of biometrics all within it. RD ensures that every device have a unique identifier allowing traceability, analytics and fraud management. Therefore, introduction of RD in Aadhaar authentication system rules out any possibility of storage and replay for biometrics. As on date, all the telecom service providers and other private entities have completely upgraded their systems to RD and other entities like banks, PDS etc. are also at various stages of implementing RD in their systems.

238

All the biometric device vendors have developed their RD services as per UIDAI specification and guidelines and accordingly their devices were certified by STQC and UIDAI for RD service. The list of the RD certified biometric devices is available at "https://uidai.gov.in/images/resource/List_of_UIDAI_Certified_Biometric_Devices_13072017.pdf"

ii. Measures taken prior to implementation of Registered Device

Following Legal, Governance and Technical measures were taken to ensure that the AUAs or AUA applications do not store biometric information collected in the process of performing authentication of residents.

- **Legal measures**

There are various measures under the Aadhaar Act, 2016 and Aadhaar (Authentication) Regulations and other regulations to ensure that AUAs do not store biometric and that they are compliant with the requirements. These are as follows:

- Section 8 (2) of the Aadhaar Act, 2016 mandates that the Identity information shall only be used for submission to Central Identities Data Repository for authentication
- Section 29 (1) & Section 29 (2) of the Aadhaar Act, 2016 prohibit sharing of biometric information and use of biometric information other than for generation of Aadhaar number generation and authentication.

- Section 37 of the Aadhaar Act, 2016 prohibits disclosure, transmission, copying or other dissemination of any identity information to a person not authorized under the Act or regulations makes it an offence punishable with imprisonment which may extend to 3 years and/or fine upto 1 lakh rupees.
- Regulation 17(1)(a) of the Aadhaar (Authentication) Regulations, 2016 specifically prohibits a requesting entity from storing, sharing or publishing for any reason whatsoever any core biometric information collected from the Aadhaar number holder and also prohibits retention of any copy of the core biometric information.
- Regulation 7(1), 7(2), 9(1), 9(5), 17 (1) (a) (b) (c) (d) (e) of Aadhaar (Authentication) Regulations mandate AUAs to secure biometric information and state how the application should process biometric information and measures against storage of biometric information
- Regulation 11 of Aadhaar (Authentication) Regulations provides a facility wherein residents can lock their biometrics as a further safeguard against misuse.
- Regulation number 14 (1) (h) of Aadhaar (Authentication) Regulations mandate yearly audit of AUA operations and systems by information systems auditor certified by a recognized body.
- Notice was issued by UIDAI dated 28-Feb-2017 reinforcing that biometrics should not be stored and replayed by AUAs

240

and mandating AUAs to submit an audit compliance certificate.

- **Governance and monitoring measures**

UIDAI has taken various governance measures to ensure that all AUAs comply with the requirements of various specifications issued by UIDAI through Aadhaar Act 2016, Regulations and other directions issued from time to time:

- AUA compliance checklist from UIDAI includes controls on prevention of biometric / PID block storage for AUAs and controls on securing authentication infrastructure with anti-virus software
- AUA Onboarding compliance audit: Before granting license key to the AUA, every AUA has to submit an audit report against the AUA compliance checklist from a third party auditor
- AUA agreement signed by the AUAs provides measures prohibiting storage of any PID information and ensuring applications are compliant to UIDAI requirement
- GRCP – Service provider of UIDAI has conducted 46 AUA audits on behalf of UIDAI to identify non-compliance with various UIDAI requirements.
- Yearly Independent Audits through CERT-IN empaneled / STQC agencies.
- Empanelment of Audit agencies: UIDAI has initiated empanelment of agencies to conduct audits of AUAs, KUAs and Sub-AUAs.

241

○ **Empanelment of Agencies for Application certification:**

UIDAI has also initiated empanelment of agencies to provide certification of applications used by various AUAs / Authentication ecosystem.

• **Technical measures**

○ **Proactive identification of Replay attacks in CIDR:** Fraud

analytics are used in UIDAI to identify replay of biometrics in CIDR. UIDAI conducts a monthly analysis on various AUAs and identifies AUAs replaying stored biometrics. Legal notices are sent periodically to the AUAs which are found to commit any violations.

○ **Biometric locking feature available to resident:** UIDAI provides a facility to the residents to lock their biometrics and prevent misuse of stored biometrics.

○ **API specification documents** of UIDAI guide the AUA organization to secure biometric / PID block at capture.

• **Trainings Workshops for AUAs**

○ Periodic workshops are held for AUAs to ensure that they are aware of the security requirements of UIDAI. Last workshops were conducted for the AUAs on 13-June-2017, 14-June-2017, 20-July-2017 and 27-September-2017.

41. It must be stated that if an entity had stored biometric illegally when the law clearly prohibits the same, then it tantamounts to theft of data and that cannot be a ground to question the law which prohibits such illegal actions. The illegal act of storage of biometrics and replay is akin to signature frauds and any offence

242

and resulting losses have to be dealt accordingly under the laws of land. Considering various kinds of impersonation frauds in online and digital world such as skimming of credit/debit cards, password attacks, signature frauds, etc. the RBI has also issued Circular as a measure of Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.

[True Copy of the RBI Circular dated 26.05.2016 and 6.7.2017 are marked as Annexure R-24 (Colly.) at Pg. 294 to 303].

42. The aforesaid RBI circular limiting liability of consumers in unauthorized electronic banking transactions would equally apply to frauds committed on Aadhaar enabled bank accounts as well.

OVERVIEW OF SECURITY REVIEW IN AADHAAR

43. The Aadhaar project is the world's largest national identity project, launched by government of India, which seeks to collect biometric and demographic data of residents and store these in a centralised database. Under the Aadhaar Act 2016, UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of Aadhaar life cycle, developing the policy, procedure and system for issuing Aadhaar numbers to individuals and perform authentication and also to ensure the security of identity information and authentication records of individuals.

243

44. UIDAI-CIDR and associated infrastructure is a Critical Infrastructure and has been declared as Protected System as per Sub-section (1) of Section 70 of IT Act 2000.
45. In reference to Sec 28 (3) of the Aadhaar Act, 2016 vide which UIDAI needs to take necessary measures to secure and protect the information stored in the Central Identities Data Repository (CIDR), UIDAI has taken a number of technical and organizational measures to continuously enhance the security of CIDR and its associated infrastructure.
46. UIDAI endeavours to continuously improve the governance and security of its design, architecture and infrastructure of internal and external ecosystem in order to stay prepared against the continuously evolving sophisticated cyber security attacks and information security threats. The present system of security and governance of UIDAI ecosystem is taken care through following Security Committees whose Roles and Responsibilities are underlined:
47. Security Review Committee was constituted to review and provide advice on Cyber Security matters for UIDAI internal and external ecosystem.

A. Aadhaar - Security Review Committee

244

- i. UIDAI has established the Security Review Committee to ensure high standards of review, governance and advice on cybersecurity, technology and privacy matters of Aadhaar.
- ii. The Security Review Committee constitutes of well recognized technocrats and professors in the country who are well known for their contributions to the field of Technology and security.

Agenda: The detailed agenda of the Security Review Committee is as follows:

i. Design

- Advise on the design of security in UIDAI ecosystem such as secure enrolment, secure authentication, secure printing, biometric processes, network architecture, encryption, and other security in CIDR etc.
- Advise on the security aspects in design of critical applications and architecture.
- Advise on research and development activities to be undertaken by UIDAI to continuously enhance the design of cyber security in the ecosystem through cyber lab / cyber center for excellence.
- Advise on the resilience of UIDAI operations and disaster recovery measures in response to cyber and physical attacks.

245

- Advise on the security technologies to be deployed by UIDAI to continuously improve the security of the ecosystem.
- Advise on proactive and detective fraud management system in the UIDAI ecosystem through appropriate policy and technology measures.

ii. Oversight and Review

- Review the threats inherent in the upcoming and existing technology.
- Provide strategic inputs on improvement in cyber security through study of major cyber-attack / fraud incidents related to critical infrastructure / National ID programs / privacy in domestic and international arena and identify gaps in the existing cyber security and cyber resilience framework.
- Provide inputs on functioning and continuous improvement of the security operations center for UIDAI ecosystem.
- Provide inputs the security impact due to significant changes in the solution / design of UIDAI ecosystem.
- Provide inputs on any technical security guidelines or standards issued by UIDAI for enhancing security of the ecosystem.

246

- Provide guidance on the response to specific security incidents / events such as ransomware attacks, malware attacks in the country etc.
- Provide guidance on the security concerns raised by stakeholders such as NCIIPC, CERT-In, STQC, GRCP, MSP, general public, Parliament, Ministry etc. through various channels such as internal/external assessments, social media, RTI, parliament questions etc.

iii. Governance

- Suggest possible policy interventions to strengthen cyber security preparedness of the UIDAI ecosystem.
- Advise on the governance measures to be taken to enhance the security of UIDAI ecosystem.
- Advise on adoption of security protocols.

iv. Composition

The composition of the Security Review Committee is as follows:

(a) Dr Ajay Bhushan Pandey, CEO, UIDAI	--- Chairman
(b) Dr. Gulshan Rai, NCSC Coordinator	--- Member
(c) Dr. Rajat Moona, Director IIT Bhilai	--- Member
(d) Dr. H Krishnamurthy, Professor, IISc	--- Member
(e) Dr. Manindra Agarwal, Professor, IIT Kanpur	--- Member
(f) Dr. Sandeep Shukla, Professor, IIT Kanpur	--- Member
(g) Dr. Subhashis Banerjee, Professor, IIT Delhi	--- Member
(h) Dr. S Rakshit, Sc-H, CAIR, DRDO	--- Member

247

(i) Dr. YLP Rao, DDG (Technology), UIDAI

Convener

[True Copy of the qualifications, background and experience of these renowned experts is marked and attached as Annexure R-25 (Colly.) at Pg. 304 to 328]

B. TARB (Technology and Architecture Review Board) :

48. TARB was constituted vide UIDAI headquarters office memorandum 18 of 2012. TARB is constituted by UIDAI to manage various aspects of Technology Layer. The Technology layer conforms to the technology aspects of the UID programme and is mainly focused on installation, commissioning and management of CIDR.
49. In 2016 a Committee of officers/representatives of UIDAI was constituted to assess the existing hardware technology with the objectives of (i) Finalization of condemnation policy for IT equipment (ii) Detail of items to be replaced/condemned out of Pre-MSP Contracts along with Quantity (iii) Item wise detail of equipment to be procured with detailed specification of hardware/software with timeline and (iv) cost Benefit analysis for the replacement/ condemned equipment.

ROLE of TARB :

- i. SLA Supervision
- ii. Compliance to Audit recommendations
- iii. Optimisation and TCO Management

248

- iv. Technology refresh
- v. Providing Micro Inputs for demand forecasting
- vi. Approval of capacity planning and cell deployment
- vii. Application enhancement and development
- viii. Management of Sub- Contractors
- ix. Usage of Open Source or free softwares

Committee Members of TARB:

(a)	Dr Ajay Bhushan Pandey, CEO, UIDAI	---- Chairman
(b)	Dr. Gulshan Rai, NCSC Coordinator	---- Member
(c)	Dr. Rajat Moona, Director IIT Bhilai	---- Member
(d)	Dr. H Krishnamurthy Professor, IISc	---- Member
(e)	Dr. Manindra Agarwal, Professor, IIT Kanpur	---- Member
(f)	DG NIC	----- Member
(g)	DG CERT-IN	----- Member
(h)	Dr. YLP Rao, DDG (Technology), UIDAI	---- Convener

50. The committee meets once in a quarter. Additional meetings are convened as per the requirement. The members of the committee outside UIDAI ecosystem sign an agreement with UIDAI to maintain the confidentiality as per the requirement of Aadhaar Act 2016 and Aadhaar Regulations. All required logistics support for the functioning of the committee is provided by UIDAI.

51. Following two external agencies are primarily responsible for conducting assessments and audits of UIDAI infrastructure and ecosystem:

249

i. Standardisation Testing and Quality Certification (STQC)

52. Standardisation Testing and Quality Certification (STQC) Directorate is an attached office of the Ministry of Electronics and Information Technology, Government of India, provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centres. The services include Testing, Calibration, IT & e-Governance, Training and Certification to public and private organizations. UIDAI has been declared ISO 27001:2013 certified by STQC with respect to Information Security which has added another layer of information security assurance. Further in pursuance of sub-section (1) of Section 70 of the IT Act 2000, UIDAI data has also been declared as Protected System by National Critical Information Infrastructure Protection Centre.
53. STQC is involved with UIDAI in various capacities. Some of the activities are mentioned below:
- UIDAI has been ISO 27001:2013 certified by STQC. The scope for assessment included the following location – UIDAI Data Centres, SOC and NOC locations and Software Development Centres.
- Qualification of auditors: Lead Auditors for ISMS and certified in ISO 27001:2013.

250

- STQC certifies the biometric devices to be used for UIDAI enrolment and authentication.
- STQC has also conducted audit of the user acceptance test for IT infrastructure procurement at UIDAI data centres.

Qualification of Auditors: Lead Auditor, Test Engineer, etc.

ii. Governance Risk Compliance and Performance Service Provider (GRCP-SP)

54. M/s PricewaterhouseCoopers Pvt. Ltd. (PwC) India has been appointed as Governance, Risk, Compliance and Performance Service Provider (GRCP-SP) since October 2015. PwC is acting as an independent monitoring agency to continuously monitor the security of UIDAI ecosystem including CIDR infrastructure, its applications, policies, processes and to monitor UIDAI ecosystem partners for compliance with the Aadhaar Act and its Regulations as well as the defined policies, procedures, guidelines among others.
55. Objective: Objective of GRCP-SP is to provide UIDAI management with oversight of security in UIDAI and security within the ecosystem partners and is expected to measure, monitor and validate that the entire ecosystem is working in a secure manner and as per the laid down regulations, policies, specifications, industry best practices etc.

251

56. Some of the important assessments and activities performed by GRCP-SP include:

- Periodic testing of all UIDAI applications using automated industry standard tools and manual testing by highly skilled technical resources
- Secure code review of all UIDAI applications
- Vulnerability assessment and penetration testing of entire UIDAI infrastructure on a periodic basis
- Network security assessments
- Review of the various security technologies deployed in UIDAI and provide improvement areas
- Review of various encryption applied in UIDAI ecosystem and its effectiveness
- Review of Database and server security
- Biometric security and de duplication assessments
- Conduct a Security gap assessment analysis of the UIDAI Information Security ecosystem.
- Information Security Policy review for the entire set of ecosystem partners of the UIDAI
- Undertake risk assessment, assess the existing controls and perform controls gap assessment
- SLA measurement framework reviews and SLA process assurance through periodic assessments for all ecosystem partners
- Conduct audits for external ecosystem partners including but not limited to Authentication User agencies (AUA), eKYC User

252

Agencies (KUA), Enrolment agencies (EA), among others.

Objective of this assessment is to enforce compliance for the ecosystem partners such as AUAs, KUAs and ASAs which use the Aadhaar Authentication services.

- Fraud risk assessment and management support

57. Further, for carrying out the above mentioned activities, GRCP-SP has deployed staff with the skillset and adequate expertise. The key roles defined are as follows:

S.No.	Profile	Area of Expertise and qualification
1	Risk Analyst	Ability to analyze technical and business risks related to security and privacy by taking into consideration multiple, global and local, trends and inputs B.E. / B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent. Preferable: CIRM / CRISC / CITR / CISSP / CISM / CBCP / GIAC / CIRCP / CIPP/IT certification or equivalent
2	Fraud Risk Analyst	Should be a seasoned fraud analyst / examiner and should have experience in handling frauds across multiple industry domains. Should be able to identify and look at a vast array of unstructured data to identify possible fraud and fraud patterns. B.E/B: Tech/B.S / MCA / M.Tech / MBA degree or equivalent. Preferable: CFS/CEH/ GIAC/ GWAPT/

253

		GWEB/ GXPN/ GPEN certification or equivalent.
3	Periodic Compliance Manager	Ability to draw up compliance schedules, compliance checklists to be followed, carrying out compliance and penetration tests, ensuring follow up for closure of identified gaps in terms of deficiencies and deviations, ensuring a regular maturity trend, keeping the team motivated B.E/B. Tech/B.S / MCA/ M. Tech / MBA degree or equivalent. Should be a certified auditor. Preferable: BS7799 Lead Auditor/ CISA/ CISM/ CISSP / CBCP / DRCS / CISRCP / CAST / GIAC/ CSCS / CBP / CBSE/ GPEN / GWAPT / GWEB / CASS / CIPP/IT certification or equivalent. ology, well versed with various tools used for protection of networks and related components from a security perspective
4	Network Security Auditor	Deep understanding of network security, protection of networks using controls related to people process and technology. B.E/B. Tech / B.S / MCA / MBA/ M. Tech degree or equivalent. Should be a certified auditor. Preferable: CISSP / BS7799 Lead Auditor/ CISM/CEH / GPEN/ GCFW/ CCNA/ CCNP/ CCSE / CCSA certification or equivalent
5	Application Security Auditor	Excellent understanding of application security and privacy impact assessment in

254

		each phase of the software development lifecycle, excellent understanding in Java security B.E/B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent Should be a certified auditor. Preferable: GWEB / CASS / GWAPT/ BS7799 Lead Auditor/ CISM / CISSP / CCSK / CIPP/IT certification or equivalent.
6	Database Security Auditor	Well versed with aspects of database security and privacy, access control, identity management, biometric storage, encryption of database, data obfuscation techniques. Has deep security related knowledge of Oracle, My SQL and SQL databases. B.E/B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent Should be a certified auditor. Preferable: BS7799 Lead Auditor/ CISSP / CISM / CISA/ CDRP/ CIRM / CBP / CBSE / CIPP/IT certification or equivalent.
7	Manager Partner Ecosystem Field Audit	Security Audits B.E. / B. Tech / B.S / MCA degree or equivalent. Preferable: CISA / CISSP / ITIL certification or equivalent
8	Partner Ecosystem Field Audit	Security Audits B.E. / B. Tech / B.S / MCA degree or equivalent.

255

		Preferable: CISA / CISSP / ITIL certification or equivalent
9	SOC Manager	Security products and technologies; security engineering, networking protocols and data center; security analysis and investigations B.E. / B. Tech / B.S / MCA / M.Tech / MBA degree or equivalent. Should be an experienced IT Security practitioner. CISSP, CISM or equivalent certification
10	IAM Manager	Requirements gathering and definition, review of security design and specification, development, testing, and implementation support B.E. / B. Tech / B.S / MCA / M.Tech / MBA degree or equivalent. Should be an experienced IT Security practitioner. CISSP, CISA or equivalent certification preferred

Security features in Aadhaar Authentication System before enactment of Aadhaar Act, 2016

58. Aadhaar authentication eco-system has been designed to ensure highest possible level of residents' data protection and security. Security was fundamental part of the authentication architecture and not an afterthought. The following security features were available before the Aadhaar Act, 2016. UIDAI strives to continuously enhance the security and privacy of Aadhaar

256

authentication through the addition of features such as registered devices, Virtual ID (VID), UID tokenization and Limited e-KYC.

59. The Aadhaar authentication is performed through multi-layered channels of trusted partners viz. Authentication Service Agencies (ASAs) and Authentication User Agencies (AUAs) having secured leased line connectivity. These partners having signed Agreements with UIDAI are bounden to comply with the provisions of the Agreement, specifications, standards, technical architecture and guidelines issued by UIDAI from time to time. All authentication related data to and from UIDAI traverse only in an encrypted form using a very high i.e. 2048 bit key asymmetric algorithm.

Security of the authentication eco-system:

- **Secure Channel:** Access to UIDAI's Central Identity Repository is available only to authorized Authentication User Agencies (AUAs), and e-KYC User agencies (KUAs) through authorized Authentication Service agencies (ASAs) which have establish secured wired network connectivity for the purpose of authentication with the Central Identities Data Repository (CIDR), in compliance with the Regulations, specifications, standards and technology architecture as prescribed by UIDAI, from time to time. Further, CIDR is accessible only through APIs defined by UIDAI and authentication request have to be in the format as prescribed by UIDAI.

257

- **Identity data is always encrypted:** UIDAI mandates that the authentication application shall immediately package and encrypt the input parameters including biometrics into personal identity(PID) block before any transmission, as per the specifications laid down by UIDAI . Therefore, resident's identity data traverse from authentication device to CIDR only in encrypted form. The Authentication request and response are always digitally signed to establish its authenticity and integrity.
- **Encrypted eKYC response :** The eKYC response is from UIDAI CIDR is always encrypted and only the KUAs ie requesting entities can decrypt it with their private keys.
- **Audit data:** The audit data containing request and response is stored for 6 months online and 5 years offline for any grievance resolution. The PID data is always kept in encrypted form in Audit.
- **Use of Hardware security module (HSM) :** All the keys are stored in secure appliance called HSM in CIDR and no key can be taken out from this appliance.
- **Use of License key by AUA/KUA/ASA:** The authorized requesting entities are allowed to generate their own license key on

258

UIDAI's portal which is part of every Auth request and is validated in CIDR before responding to Auth requests.

- **STQC certified biometric devices:** UIDAI has mandated use of only Standardisation Testing and Quality Certification (STQC) certified biometric devices for all authentication requests.
- **Multi-factor authentication:** UIDAI provides multiple ways of authentication such as demographic, biometric (Fingerprint/Iris), OTP or a combination of these factors. Further, the Authentication User Agency may decide to use additional authentication factors on their own depending on their security need and business requirements.
- **Biometric locking:** Some residents might be having the apprehension that any unscrupulous element may capture their biometrics (Fingerprint / Iris) and use it for fraudulent Aadhaar Authentication. UIDAI has provided the facility to protect against an eventuality whereby residents can lock their biometrics and whenever they need to do Aadhaar authentication using biometrics, it can be unlocked for a specified short period of time.
- **Alert notifications:** UIDAI provides instant e-mail alert notifications to Aadhaar number holder for biometric authentication with details such as time of authentication, mode of authentication, the name of Authentication user agency through which

259

authentication has happened, UIDAI's response (Yes or no) and contact details of UIDAI. Therefore, in case of any issues with the transaction, Aadhaar number holder may approach UIDAI or the Authentication user agency.

- **Fraud detection and prevention:** UIDAI keeps on doing analysis on the transactions performed by various AUAs and based on the requirement keeps on adding new features or rules to ensure increased security of authentication transactions. AUAs are also advised to perform analysis on the transactions to monitor and avoid any irregular or fraudulent activity

60. It is submitted that Professor Manindra Agarwal of IIT Kanpur, a renowned computer scientist and the recipient of the famous Godel Prize in Computer Science has analyzed the major concerns relating to the Privacy and Security of Aadhaar. After a comprehensive examination, he has concluded in his Report that Aadhaar brings significant benefits to our society without any further reduction in security and privacy and that none of the concerns raised by the Petitioners with respect to Aadhaar compromise Privacy or Security.

[A True Copy of the Report titled "Analysis of Major Concerns about Aadhaar privacy and Security by Prof. Manindra Agrawal" is attached as Annexure R-26 at Pg. to .]

61. It has been argued by the Petitioners that as a centralised database, Aadhaar is vulnerable to attack.
62. The allegation is vehemently denied for the following reasons:

63. The CIDR has been designed so that it is bifurcated into two distinct systems - the Authentication system and the Enrolment system. Only encrypted data from registered operators of enrolling agencies are allowed to enter the Enrolment System, after passing a rigorous check at the firewall surrounding this system. This firewall acts like a one-way software valve and ensures that data can only enter but cannot leave.
64. The resident data packets are transported in encrypted form until it passes through the firewall within the physical premises of the CIDR. This encrypted data can only be decrypted by the Hardware Security Module (HSM) that is physically located inside the CIDR. The HSM is completely isolated from the public internet. It is designed to self-destruct if any attempts are made to attack it.
65. The Authentication system allows for two-way traffic to and from the CIDR. However, authentication can only be carried out on requests initiated by AUAs or KUAs who in turn cannot directly access the database but have to do so through the infrastructure provided by ASAs. These ASAs maintain dedicated infrastructure solely for the purpose of connecting the AUAs to the Aadhaar database. Thus, access to the Authentication CIDR is not available over the public internet. The UIDAI has created a private network for the purpose of accessing the Authentication CIDR. Access to this Aadhaar internet is limited to only registered entities and all authentication transactions that take place on it are logged and capable of being attributed. As a result, this system is secure from attacks through the public internet.

261 —

66. All devices that collect biometric or demographic information must be registered with the UIDAI and the CIDR will refuse to accept authentication requests made by requesting entities using unregistered devices. All communication to and from the CIDR database is encrypted with a high level of encryption making it impossible for any third party to read any of this information. The entire CIDR system is maintained in a highly secure physical environment with high security and very limited access being allowed into the premises.
67. Petitioners have alleged that Aadhaar could result in Impersonation of People using their Biometrics.
68. The said fear and concern is unfounded and Aadhaar does not add to the security concerns in any which way.
69. Biometric authentication can only be carried out using registered devices in presence of the operators authorized by the requesting entities. In the event any impersonation is carried out using "gummy fingers" or any of the other mechanisms suggested by the petitioners it will be detected by the operator of the requesting entity in front of whom the biometric authentication is being done. Therefore, the only way in which an individual may impersonate another person using the latter's artificial biometrics is with the collusion of the operator of the registered device. In a non-Aadhaar enabled banking transaction, a fraud can be committed with the collusion of the banking official and therefore the technology cannot be questioned on that count.

262

70. Additionally, the UIDAI has implemented a feature whereby biometrics can be locked. In such event the use of these features will be precluded since the user will have to first unlock the biometrics on the UIDAI portal before the artificial biometrics can be used by the person seeking to impersonate the resident.
71. The UIDAI has already announced the implementation of a Virtual ID system that will allow every Aadhaar number holder to create unique virtual ID numbers that can be used instead of their Aadhaar number. This means that in the future, there will be no need to disclose your Aadhaar number in any transaction unless the requesting entities have been specifically mandated to collect Aadhaar number under the law..
72. Another allegation leveled by the Petitioners is that the Government is not involved in the Enrolment Process leaving the enrolment data vulnerable in the hands of the private players.
73. Firstly, this assertion is not correct. A large number of enrolments have been carried out directly by the Registrars i.e. the State Government or State instrumentalities wherein even though enrolment are carried out through private entities, the Registrars maintain a high degree of control over the entire enrolment process. The enrollment is done using standardized software provided by UIDAI where every keystroke of the operator is audited. The operators that carry out the enrolment are required to undergo a training by an agency empanelled by the UIDAI and are required to

263

pass an exam before they begin enrolment. Every operator who enrolls a resident is required to authenticate each individual enrolment record using their own biometrics to ensure that the UIDAI has an auditable trail of each enrolment that has been completed. Accordingly, any deviations from the standards prescribed the UIDAI are immediately recognized and action taken.

74. The enrolment system has been designed so that from the moment the biometrics have been captured, enrolment packets are encrypted within the enrolment client and are only be decrypted when they reach the CIDR. At this point in time, the enrolment packet is entirely within the control of the government. Thus, even though private entities are used to carry out the enrolment activities, the system has been designed so that nowhere along the way will any private entity get access to an individual's biometrics.
75. The Petitioners have alleged that the security of the data will be compromised on account of the involvement of foreign parties.
76. The said allegation is denied as incorrect and completely misplaced. The only foreign parties that were ever involved in the Aadhaar system were entities that carried out the de-duplication process within the CIDR database. Since biometric authentication needed considerable technical expertise to carry out accurately, the UIDAI engaged the companies with the best biometric de-duplication solutions in the world to carry out the de-duplication. In order to ensure the safety of the biometric information, the UIDAI implemented various safeguards to ensure that these companies do not have access to any Aadhaar information.

264

77. In order to carry out de-duplication, the deduplication software of these Biometric Service Providers (BSPs) which were installed on the UIDAI's servers inside its secure datacenter were only provided with the biometric images and corresponding reference numbers to compare against their existing database of biometrics. No other information - demographic or otherwise (and in particular no names) were provided to the biometric deduplication system of the BSPs. Accordingly, there was no way for Biometric Deduplication system to co-relate a set of biometrics to any particular resident.
78. In any event, all de-duplication activities of BSP systems took place within the physical location of the UIDAI Datacenter. They were carried completely isolated from the public internet. There was no possibility for for BSPs to leak any biometric data to the outside.
79. That the Petitioners have leveled allegations that the contract agreement entered into between the Answering Respondent and M/S L1 Identity Solutions Operating Company Pvt. Ltd. who is the biometric solution provider (BSP) for the purpose of de-duplication has led to a security concern and it has been alleged that the biometric of all Indians have been parted with to M/s L1 Identity Solutions Operating Company Pvt. Ltd.
80. The above allegation is vehemently denied as being incorrect and contrary to the factual position. It is submitted that the Answering Respondent has only taken software services for a limited purpose of de-duplication from M/s L1 Identity Solutions Operating

265

Company Pvt. Ltd. The said software is run on the Answering Respondent's proprietary servers at the data centers owned by the Respondent herein. There is only a limited technical staff of M/S L1 Identity Solutions, which is stationed outside the server area in the Data Centre of UIDAI. This technical staff intervenes only when some snag is noticed in the software functioning. When the technical staff is required to carry out corrective measures, they are done under the supervision of the UIDAI officers. None of these technical staff of M/S L1 Identity Solutions are allowed any access at will in the area where the servers are located or where the data is stored. In fact this limited staff has no role to play even in de-duplication which is done automatically by the software. Additionally, the Data Centre is guarded by armed 24/7 by CISF Security personnel and is also supervised by UIDAI officials.

81. As an additional safeguard, the biometrics, which is run on the software for de-duplication, is completely anonymised and no demographic data is shared which would enable the software to know whom the biometrics belong to. Only a reference ID is given against the Biometric, the corresponding details of which are known only to UIDAI.
82. It is reiterated that no Biometric data is given to or stored with M/S L1 Identity Solutions and the biometrics are only processed on L1's software on UIDAI's owned servers with CIDR for the purpose of de-duplication and generation of Aadhaar Numbers. It is further reiterated that M/S L1 Identity Solutions cannot take out the data or store it with them in any manner whatsoever. Even after the

266

term of the Contract, M/S L1 Identity Solutions cannot take away the biometric data or access the same in any manner whatsoever.

III. ALLEGATIONS DEALING WITH PRIVACY & SURVEILLANCE

83. The allegations relating to breach of privacy and possibility of surveillance have already been dealt with and controverted by the answering respondent in earlier Common Additional Affidavit dated 15.01.2018 filed by it at Paras 78 to 89 at Pages 70 to 77. Additionally, it is submitted

Brief Note on Meta Data refuting the allegations of the Petitioners

84. The Petitioners have alleged that the collection of Meta-Data envisaged under Regulation 26 of the Aadhaar (Authentication) Regulations, 2016 is the main concern with respect to the privacy challenge to the Aadhaar Act, 2016. It has been argued by the Petitioners that the meta-data stored and collected by the Authority will enable the Government and/or the Authority to know about the purpose of the authentication as well as the location of the authentication and thereby lead to surveillance.

267

85. At the outset, it is vehemently denied that either the purpose of authentication or the location of the authentication will be known to UIDAI or the Government of India.
86. Section 32(3) of the Act categorically prohibits the Authority, either by itself or through any entity, to collect, keep or maintain any information about the purpose of authentication and therefore the Authority is by design and by law completely blind to the purpose for which authentication may be done by an individual.
87. It is submitted that even the location of the authentication will not be known or collected by the Authority. The only information that the UIDAI maintains with respect to an individual's authentication transactions are - the time of authentication, the requesting entity that carried out the authentication and the response provided by the CIDR to this authentication request. The CIDR does not maintain, or even have the ability to maintain, information with respect to the location where the authentication was carried out or the specific reason for the transaction and for which entity. The UIDAI is precluded by law from maintaining any information with respect to the purpose of the authentication.
88. Therefore, from the information actually available with the UIDAI it is impossible for the UIDAI to carry out any form of surveillance that will allow it to ascertain on a daily basis, the movements of an Aadhaar number holder or carry out surveillance activities in any

other way. Additionally, neither the AUAs nor the KUAs, that process the authentication request, maintain any GPS location data and therefore do not conduct any real time surveillance of any individuals using the Aadhaar authentication ecosystem.

89. A fear has been expressed that when the Aadhaar number is mandatorily required to be linked to a database (including private sector databases such as banks and telecom companies) and that merely by linking the Aadhaar number, the government has the ability to discern an individual's transactions with those companies. In other words, the fact that the database now includes the Aadhaar number somehow gives the Government the ability to monitor the activities of the resident with those companies. The said allegation is completely denied as incorrect and false.
90. When the Aadhaar number of a resident is added to the database of a telecom company the telecom company now has simply verified the identity of the Aadhaar number holder against the central identity database. However, the CIDR has no information about the many ongoing transactions that the individual undertakes in connection with the services that the telecom company provides him. From time to time the telecom company might require to authenticate its subscribers and for this purpose will use the authentication facility to do so. However, as described earlier, no such authentication contains location data or the purpose for which the authentication is being carried out – without which surveillance

as feared is not possible. It is therefore impossible for the government to maintain a central database of the physical location and activities of individual as alleged by the Petitioners.

Location of Registered Devices

91. The Aadhaar authentication system does not collect and store the location information about the place where the authentication is being carried out. As is evident from the latest version of the technical documentation relating to the Aadhaar authentication Application Programming Interface (API), the location of the registered device is not submitted as part of the authentication process.

There is nothing contained in the API that would provide any indication of the location of the device at the time of authentication. Owing to the mobile nature of such devices, it would make it very difficult to locate where exactly the authentication was carried out.

92. A more detailed and elaborate discussion on the nature of meta-data collected is provided hereinafter.
93. A requesting entity performing Aadhaar authentication using demographic, biometric or OTP mode of authentication shall send request to UIDAI as per Aadhaar Authentication API and e-KYC API. 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-

270

KYC API (v2.1). In addition, UIDAI does not receive any information about the device operator details and the purpose of authentication.

94. Authentication API contains the following elements:
1. **Auth element** contains attributes: UID number, Resident Consent, tid (For Registered devices, value is "registered", blank in case of non biometric authentication), AUA Code, Sub AUA Code, Version of API, AUA specific Transaction identifier, License Key
 2. **Uses element** specifies the authentication factors used in the request.
 3. **Meta element** specifies meta data related to the device. This element contains the following attributes:

S.No.	Attribute Name	Brief Description
1	Udc	Unique Host Device Code. This is a unique code for the host device, assigned within the AUA domain. This may be used by the AUA for audit purposes, performance (biometric capture quality) improvement and fraud analytics at the device level. UIDAI does not receive information (such as IP

271

		address etc.) which may be used to identify the location of the device, device operator details or purpose of authentication.
2	dpId	Unique ID assigned to registered device provider. This ID is the same for all the devices from the same device provider.
3	rdsId	Unique ID of the certified registered device (RD) service. The ID is the same for each device using the same RD service.
4	rdsVer	RD service version number. The version number is the same for all devices using same version of the RD service
5	Dc	Unique Registered Device Code. The registered device code specifies the ID associated with a biometric authentication device. This is required for audit purposes audit purposes, performance (biometric capture quality) improvement and fraud analytics at the device level. UIDAI does not receive information such as IP address or GPS location which may be used to identify the location of the device. UIDAI does not receive device operator details or purpose of authentication.

272

6	Mi	Registered device model ID. The model ID is identical for all devices of the same model.
7	mc	This attribute holds registered device public key certificate, signed with device provider key. This certificate allows UIDAI to verify that the biometric has been captured live on registered biometric device.

UIDAI only gets unique device code and registered device code which are used for audit purposes, performance (biometric capture quality) improvement and fraud analytics.

4. **skey element** is for session key. ci parameter in skey element is Public key certificate identifier using which "skey" was encrypted.
5. **Data element** contains encrypted PID block having demographic, biometric or OTP data of the Aadhaar number holder for performing the authentication.
6. **Hmac element** contains the hash value of the PID block.
7. **Signature element** is the signature of the requesting entity which ensures that request XML should be digitally signed for message integrity and nonrepudiation purposes.

95. The e-KYC API contains the following additional elements:

1. **Kyc element** is Root element of the input XML for e-KYC API.

This element contains the following attributes:

- a. Version of eKYC API

273

- b. resident authentication type
 - c. Resident's explicit consent for the transaction
 - d. Request for data in local language
 - e. Delegation of decryption to ASA by KUA (based on UIDAI approval)
 - f. Format of the response data (pdf/xml)
2. Rad element contains the base64 encoded fully valid Auth XML for resident.

96. As per Regulation 18(1) of Aadhaar (Authentication) Regulations, 2016, "a requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:—

- (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."

UIDAI does not ask requesting entities to maintain any logs related to IP address of the device, GPS coordinates of the device etc.

97. As per Regulation 18(4) of Aadhaar (Authentication) Regulations, 2016, "*The requesting entity shall not share the authentication logs*

274

with any person other than the concerned Aadhaar number holder upon his request or for grievance redressal and resolution of disputes or with the Authority for audit purposes. The authentication logs shall not be used for any purpose other than stated in this sub-regulation."

98. Further, as per Regulation 26(1) of Aadhaar (Authentication) Regulations, 2016, UIDAI shall not store the purpose of authentication. UIDAI can only audit the authentication logs maintained by the requesting entity as per Regulation 18(1) of the Aadhaar (Authentication) Regulations, 2016.
99. It may be noted that previous versions of the Aadhaar 1.6 version API had fields corresponding to the public IP address if available, and a location value which could either be a PIN code or GPS co-ordinate. The default value of "NA" for the public IP and a static PIN code for location was used for a vast majority of applications since there was no way to validate this data at the backend. This data cannot be used for surveillance purposes. These fields have been subsequently removed from the Aadhaar API (in November 2016) to remove even the possibility of misuse in the future, and ensure strict compliance with the Aadhaar Act. Subsequently, these parameters were removed from the Authentication API 1.6 in November 2016.
100. Therefore, UIDAI cannot obtain the location and purpose of authentication and the argument that there will be an electronic trail

275

which will enable the State to do surveillance is completely incorrect and denied. Not only is surveillance not the object of the Act but to impute mala fides on the legislative intent and Parliament is legally untenable and unacceptable. It is equally unacceptable to use expressions like "Surveillance State", "Electronic leash" and "totalitarian government" without any factual basis.

101. It is reiterated that Aadhaar is not a tool for surveillance. The project provides for good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto.

Reply to the Affidavit of Mr. JT D'souza

102. That the Petitioners have filed an Affidavit of one, Mr. JT D'souza dated 22.11.2016 through IA No. 94343/2016 in W.P.(C) No. 797/2016 filed on 16.12.2016. By way of this Affidavit, Mr. JT D'Souza has contended that fingerprints are unreliable and that fingerprints can be replicated using materials widely available in the market.
103. It is submitted that contentions of the Mr. JT D'souza are incorrect and denied. It is denied that fingerprint can be replicated and

276

misused for authentication. It is submitted that fingerprint authentication under the Aadhaar project is conducted through an assisted model, i.e., in the presence of authorized representatives of AUA/ASA, thereby dissuading fraudulent activities.

104. That the contents of Para 5 of the Deponent's Affidavit are denied as being false, baseless and a misrepresentation of the facts on record. As a matter of policy and by design, the UIDAI precludes itself from aggregating information arising from the use of Aadhaar, tracking and profiling individuals. The system by intent is blind to the purpose for which Aadhaar may be used at the front end by the resident. Aadhaar is designed on the basis of principles of "Minimal Data, Optimal Ignorance, and Federated Database", which will prevent UIDAI, Government or for that matter any Department or Agency to track and profile any individual. For example, a person may use his Aadhaar number for obtaining a SIM card, opening a bank account, and receiving his PDS benefits. Even though Aadhaar number is used by the individual for all the three purposes, a telecom company will not have any information about his bank details or PDS benefits received by him. Similarly, the bank will not know his SIM cards details and his PDS benefits. So far as UIDAI is concerned it will not have any of the three information— bank details, SIM cards details, and PDS benefits details. A user department of the government, or agency will have information pertaining only to its own domain and will never have or will not be able to build a 360 degree view of any of its

277

customers or beneficiaries. These principles of Optimal Ignorance, Minimal Data and Federated Databases have now been codified by the Parliament in the Aadhaar Act, 2016 itself. It is further submitted that a para-wise reply to the contentions raised by the Deponent in Para 5 are as follows:

- a. That the Contents of Para 5 (a) are false, baseless and misleading. It is submitted that UIDAI never mandated the use of GPS devices or technology for the purpose of authentication. UIDAI has always published its APIs (Application Programming Interface) in public domain for transparency purposes. As per the applicable Aadhaar Authentication API there is no parameter to capture the location of authentication through IP address, GPS, Geo-location or any other location based specification. Also as per Regulation 26 of Aadhaar (Authentication) Regulations, 2016, UIDAI shall not, in any case, store the purpose of authentication.
- b. That the contents of Para 5(b) are incorrect and a misrepresentation of the facts on record. It is submitted that Registration of device and assignment of unique device code does not mean tracking of the exact place of the transaction. Registration of device and assignment of unique device code is done to protect the privacy of the residents, and to detect and prevent fraudulent transactions. This device code does not have location information. All that the UIDAI is capturing is the Unique Device Code and Unique Registered

270

Device Code which are merely Unique code of devices of a particular entity and as per authentication API, UIDAI does not capture location parameters and IP address of authentication device.

- c. That the Contents of Para 5(c) are denied as being incorrect and misleading. It is submitted that UIDAI cannot determine the authentication location or conduct real time surveillance as it does not obtain IP address, GPS or any other location based information. UIDAI has always published its APIs in the public domain for transparency purposes and the APIs do not have the capability to collect such data.
- d. That since the UIDAI is not capturing device location, GPS co-ordinates, IP address of device and purpose of Authentication, hence it is not possible for UIDAI to trace the transaction of any Aadhaar Number holder and to create the profile of Aadhaar Number Holder. Therefore the apprehensions and allegations to this effect are baseless. UIDAI is capturing unique device code and unique registered device code which are merely the identity code of devices of particular entity. This is done to protect the privacy of the residents, and to detect and prevent fraudulent transactions. Hence, UIDAI cannot track the location of authentication.
- e. That the contents of Para 5(d) are denied as being false. It is submitted that Aadhaar verification ecosystem is designed to preclude surveillance of any nature. Current data collection of UIDAI does not have any capability to collect data that

279

can be used for surveillance and is based on optimal ignorance principle. Additionally UIDAI cannot collect data that potentially may be used for surveillance in future as the Aadhaar Act provides for various protections against any violation of privacy. The Aadhaar Act of 2016 and Regulations prohibit use of any identity information for any purpose other than authentication and generation of Aadhaar number.

- f. That the Contents of Para 5(e) are denied as being false and a misrepresentation of the facts on record. For the sake of brevity the contents of the aforesaid submissions are reiterated herein to submit that the Mr. JT D'souza's example of surveillance at the time of boarding at an airport, collecting rations at a PDS fair-price shop or withdrawing money from an ATM machine are not possible as UIDAI does not capture such information nor is it permitted under the law to do so.
- g. The Contents of Para 5(f) are denied as being incorrect. It is submitted that UIDAI has always published its APIs in the public domain for transparency purposes. UIDAI authentication API does not capture any IP address of any communicating device. All biometric devices used for authentication, communicate on USB port, with parent machine, do not have IP address and therefore capturing of IP address of biometric devices such as finger print reader does not arise. All biometric devices used for authentication

280

- are registered with UIDAI by OEM and are called as registered devices.
- h. That the AUAs decides the mode of communication between their servers and Registered Devices (as prescribed by UIDAI) which could be USB (universal serial bus) or TCP (IP) or any other appropriate protocol. The location of AUA/ASA server can be located but the place of authentication cannot be tracked by UIDAI. The UIDAI neither gets IP address of the device nor does it capture the IP address in the entire authentication chain. Therefore the contention of deponent that it is easy for UIDAI to locate the place of authentication transaction is false.
- i. That UIDAI collects minimal data which is required to maintain the necessary audit trail. This data does not capture any IP address. Any authentication request to UIDAI comes from the Authentication User agency (AUA) and UIDAI only stores the necessary details of the AUA which does not include the IP address or GPS location. Each part of the electronic path is maintained by AUA and each one of them is under the obligation of their parent law to maintain confidentiality and prevent unauthorized disclosure / recreation of path.
- j. The intermediate servers or telecom service provider or banking may store other details of the transaction as per the requirement of their parent Act. UIDAI does not have any control or access to such details. Therefore the location of

201

authentication is not possible and hence it is denied that UIDAI will be able to track the electronic path.

- k. That the Contents of Para 5(g) are denied as being false and misconceived. It is submitted that Aadhaar is more secure than any other alternatives present. For example, it is possible to forge someone's signature and withdraw money through withdrawal slips or a cheque book or to carry out an internet banking transaction with compromised password. UIDAI has established strict controls to avert any fraud. It is stated that UIDAI has mandated use of registered device where each finger print captured is encrypted with UIDAI key with time stamp. All the devices used are STQC certified whereby it is ensured that no storage is possible and no facility of connecting alien external devices is provided since it is a sealed device.
- l. That the Contents of Para 5(h) are false, baseless and misconceived. It is submitted that there is no substantiated proof for existence of such risks in the hardware and software manufactured by overseas corporations. Without prejudice to the above, even if such risks exist, UIDAI has taken risk-minimizing measures. It is submitted that UIDAI has deployed a robust certification process to ensure that the devices used in the UIDAI ecosystem are free of such risks. The devices used by UIDAI are STQC certified devices and it is mandated under the Aadhaar Act for all enrolling

282

agencies and requesting agencies to use only STQC certified devices.

m. It is submitted that even Defence Organisations procure systems from foreign vendors and even they may face similar possibilities. Therefore, even their equipment is subjected to certain testing, by certified agencies. Similar system of certification is followed by UIDAI. It is submitted that across the world no country is capable enough to produce all equipments indigenously required for their operations. Risks associated with foreign vendors are controlled using standard certification processes and monitoring and other risk mitigation measures.

n. That the Contents of Para 5(i) is denied as being false. It is submitted that the authentication data remains with the requesting entity which performs authentication for service delivery. UIDAI does not capture the location, purpose, profession etc. of any Aadhaar number holder performing authentication, therefore UIDAI cannot create profile of any Aadhaar number holder and cannot compromise the privacy of Aadhaar number holder.

105. That Mr. JT D'souza in Para No. 7 of his Affidavit has contended that using modern photography instruments, it is possible to replicate irises and use those false copies for purpose of authentication. It is submitted that UIDAI has also mandated to use Registered Devices (RD) in case of Iris devices. With Registered

Iris 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/iris image and replay of biometrics / iris image captured from other source.

106. That UIDAI provides instant e-mail alert notifications to Aadhaar number holder for biometric authentication with details such as time of authentication, mode of authentication, the name of Authentication user agency through which authentication has happened and contact details of UIDAI. In addition, Aadhaar number holder may view the "Authentication History" i.e. details of the transactions performed by him / her in the last few months by entering Aadhaar number and OTP verification through registered mobile number.
107. That further, as a measure of enhanced security, biometric lock feature is also provided, wherein UID holders can lock / unlock their biometrics as per their requirement. Authentication in UIDAI is through an assisted model which dissuades a fraudulent activity. Use of false iris copies for authentication would require collusion with AUA operator. Any such act is punishable under Aadhaar Act, 2016.

108. That Mr. JT D'souza, in Para No. 8 of his Affidavit has contended that the implications of using Biometrics as an authenticating factor is akin to 'walking around with your password painted on your forehead' based on the examples of cracking of the I-phone Biometric Authentication. It is submitted that such an allegation is misplaced and completely denied. UIDAI has established adequate controls to prevent against such possibilities. These controls include registered devices, biometric locking, multi-factor authentication, resident notification and Aadhaar number locking. In addition, Authentication in UIDAI is through an assisted model which dissuades a fraudulent activity. Use of false iris copies for authentication would require collusion of AUA operator and any such act is punishable under Aadhaar Act, 2016. That apart from the capability of preventing such possibilities, UIDAI has built systems based on fraud analytics to be able to detect any such occurrence of suspicious activities. UIDAI offers a much more secure method of authentication than the traditional systems and technologies prevalent before UIDAI which have proven to be filled with multiple possibilities of fraud already and UIDAI, through technology, is offering the most secure means of identity verification.

Reply to the Affidavit of Mr. Samir Kelekar

109. That the Petitioner in W.P.(C) No. 797/2016 have filed an Affidavit in the name of Mr. Samir Kelekar dated 06.04.2016. Mr.

205
31

Kelekar has deposed in his Affidavit that the Aadhaar Project is highly imprudent as it throws open the clear possibility of compromising basic privacy of facilitating real-time and non real-time surveillance of UID holders by the UIDAI and other actors that may gain access to the Authentication Records held with UIDAI or the Authentication data traffic itself.

110. It is submitted that the averments made by Mr. Kelekar are denied as being false, baseless and unsubstantiated. It is denied that the Aadhaar project poses a constitutionally impermissible danger to citizens' basic civil liberties including their privacy. In fact UIDAI has learnt from the defects of other National ID programs and has ensured privacy by design through minimal data collection and no tracking or profiling. It is submitted that the entire Aadhaar Act of 2016 has been drafted keeping an eye on the privacy of the individual which permeates the entire legislation. Certain provisions of the Aadhaar Act, 2016 to this effect are enlisted below to corroborate the above submission.

- a. Section 2(k) contains the definition of demographic information and that such information shall not include race, religion, caste, tribe, ethnicity, and language, records of entitlement, income or medical history.
- b. Section 3(2) requires the enrolling agency to inform the resident the manner in which the information shall be used and with whom the information will be shared.

- c. Section 4(2) requires Aadhaar to be a random number which bears no relation to the attributes or identity of the Aadhaar number holder. This is important because even the US Social Security Number, for example, has enough of a pattern that an expert can guess a person's number from their birth date and from the location at which it was issued. But any such possibility is avoided with a 12 Digit random Aadhaar number.
- d. Section 8(2)(b) requires that the identity information of an individual is only used by a requesting entity for submission to the CIDR for the purposes of authentication.
- e. Section 8(4) limits the Authority to respond to an authentication request with a positive, negative or any other appropriate response sharing such identity information, excluding any core biometric information. That is, under no circumstances would the UIDAI share with any requesting entity any core biometric information defined in Section 2(j) being the finger prints or Iris scan.
- f. Section 28 requires the Authority to ensure security of identity information as also the authentication records and also subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records. Section 28(5) also prohibits any officers or employees from revealing any information in the CIDR whether during service or thereafter.

- g. Section 29(1) contains a complete prohibition from sharing of core bio-metric information. Section 29(2) states that other identity information may only be shared in accordance with the provisions of this Act and Section 29(3) states that no such identity information available with a requesting entity shall be (i) used for any purpose other than that specified to the individual at the time of submitting such identity information for authentication (embodying the privacy principle of purpose limitation); (ii) disclosed further, except with the prior consent of the individual to whom such information relates. Section 29(4) states that no Aadhaar number or core biometric information shall be published, displayed or posted publicly.
- h. Section 30 states that biometric information shall be deemed to be sensitive personal information under the IT Act, 2000 and all the safeguards and provisions and the rules made thereunder are made applicable.
- i. It is also pertinent to note that Section 32(3) of the Aadhaar Act, 2016 specifically prohibits the UIDAI from controlling, collecting, keeping or maintaining any information about the purpose of authentication either by itself or through any entity.
- j. That it is also pertinent to note that no requesting entity can store and use the biometrics taken at the time of Aadhaar authentication. The biometrics are encrypted as soon as Aadhaar holder places his finger on fingerprint sensor and

288

this encrypted data is sent to UIDAI for verification. Regulation 17(1)(a) of the Aadhaar (Authentication) Regulations 2016, strictly prohibits any requesting entity which includes mobile phone companies, banks etc from storing, sharing or publishing the finger-prints for any reason whatsoever and neither shall it retain any copy of such finger prints. Any violation of this provision is a punishable offence under the Aadhaar Act 2016.

- k. Section 33(1) provides for limited disclosure of identity information other than core biometric information only subject to Court order by a Judge not below the rank of a District Judge.
 - l. Section 33(2) provides disclosure only in the interest of national security and only upon a direction by an officer not less than the rank of a Joint Secretary which is further 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 (now, Ministry of Electronics and Information Technology), before it takes effect.
111. It is humbly submitted that therefore, at every step, the privacy of the individuals has been given protection. That to further strengthen the privacy and security of Aadhaar number holders, UIDAI has introduced additional features in the form of Virtual ID (VID)

209 —

service vide Circular No. 1 of 2018, dated 10.01.18 bearing F. No. K-11020/217/2018-UIDAI (Auth-I) issued by the UIDAI.

112. That it is denied that the Aadhaar project is imprudent with the possibility of facilitating real-time and non real-time surveillance of UID holders by the UID Authority and other actors that may gain access to the authentication records held with the Authority or authentication data traffic. It is submitted that as per the present and currently applicable Aadhaar Authentication API (Application programming interface) there is no parameter to capture the location of authentication, IP address, GPS or any other location based specification. These APIs have always been published on the Internet by UIDAI to create transparency in the data collection practices. Further, Regulation 26 of Aadhaar (Authentication) Regulations, 2016 permits UIDAI to store and maintain limited data in respect of the authentication transactions which is restricted to (a) authentication request data received including PID block; (b) authentication response data sent; (c) meta data related to the transaction; and (d) any authentication server side configurations as necessary. UIDAI is expressly prohibited from storing the purpose of authentication under Regulation 26 of the Aadhaar (Authentication) Regulations, 2016.
113. That Mr. Kelekar, in Para 9 of his Affidavit, has contended that it is easy to know the place and type of transaction every time such authentication takes place using a scanner for fingerprints or iris. It

290

is humbly submitted that the contents of Para 9 are baseless, misleading and false. It is denied that it is possible to know the place and type of transaction every time such authentication takes place using a scanner for fingerprint or iris and the records of these is in the Aadhaar/UID Database. Authentication APIs (Application programming interface) have always been published in the public domain by UIDAI to create transparency in the data collection practices. As can be seen from the APIs, they do not have any capability to collect the place or type of transaction. Section 32 of the Aadhaar Act, 2016 prohibits the Authority, either by itself or through any entity under its control, to collect, keep or maintain any information about the purpose of authentication. The transaction details with regard to purpose, amount, place etc. may however be maintained by the concerned AUA/KUA as per their contractual obligations with their licensing authority or as per the respective laws. It is pertinent to mention here that such records would have been maintained by the AUA/KUA even if any other method of authentication (other than Aadhaar based authentication) was used and all such records are required to be secured by the AUAs/KUAs. Additionally, UIDAI has no control or access over such data maintained by these agencies.

114. That further, the submission made by Mr. Kelekar in Para 10 and Para 13 of his Affidavit are denied as being incorrect, baseless and a misrepresentation of the facts on record. It is humbly submitted that UIDAI does not require the biometric scanners to bear any

291

specifications in respect of IP address, GPS or any other location based technology. It is further clarified that the UIDAI does not obtain the physical location of the authentication transactions through the IP address of the scanners.

115. Authentication APIs do not capture any IP address of any communicating device. Assignment of unique device code and registration of devices by UIDAI does not mean tracking of the exact place of the transaction. Registration of devices and assignment of unique device codes are done to protect the privacy of residents, and to detect and prevent fraudulent transactions. Such unique device code cannot be construed as trackers as the device codes do not contain any location based specifications. Further, such devices are portable and not restricted to a predetermined or specified location.
116. That lastly, the information received by UIDAI for the purpose of carrying out authentication transaction does not contain the location of the device or the transaction. Therefore, it is impossible for the UIDAI to identify the location of the device or the authentication transaction conducted through the device. Since no such information is maintained or stored with UIDAI itself, the same cannot be obtained by any person, entity or authority through UIDAI's system.

117. That in Para 11 of his Affidavit, Mr. Kelekar has deposed that there are technical tools that are available which make it easy and possible to track the electronic path that authentication requests take from any given authentication device to the Central Identification Data Repository. It is humbly submitted that the aforesaid contention of the Deponent is denied as being false and baseless. Each part of the electronic path is maintained with the respective service providers such as AUA or the telecom companies and each one of them are under the obligation of their parent law to maintain confidentiality and prevent unauthorized disclosure of path. The intermediate servers or telecom service provider or banks may store other details of the transaction as per the requirement of their parent Act. Therefore, the location of authentication is not possible unless the UIDAI, government agencies, Internet service providers, AUAs/ASAs etc. together connive to breach all laws and contracts.
118. That in Para 12 of his Affidavit, Mr. Kelekar submits that since no security is perfect, A system must be designed where in case of a breach, the damage is minimal and backups are available. According to Mr. Kelekar, for the aforesaid reason, passwords should be changeable and Biometrics as a password is problematic as they cannot be changed if stolen/lost or hacked. It is submitted that the aforesaid contention of Mr. Kelekar is denied as being false, misconceived and the result of a lack of understanding of the mandate of the Aadhaar Act. It is submitted that under the Aadhaar

293

Act, Biometrics are not being used as a password. It is merely used for authentication/identification of a person and not for authorization of transactions.

119. It is reiterated that the basic purpose of Aadhaar is to confirm the identity of the person to whom the benefit is targeted to be given. Aadhaar is a very effective instrument of de-duplication because of biometrics as it is almost impossible for one person to obtain two Aadhaar numbers, therefore entry of fake and duplicate beneficiaries into any scheme can be checked through mandatory use of Aadhaar. During the last 70 years, all attempts to weed out bogus and duplicates from welfare schemes such as PDS, MNREGA etc through other methods turned out to be futile. Since, now the benefits will be distributed through Aadhaar authentication, it will be much harder to fudge records showing distribution to fake and duplicates and deny the genuine beneficiaries. Under the Aadhaar regime everyone involved in the delivery system is subjected to a greater accountability and on the other hand, citizen is empowered because it is harder for anyone else to impersonate him and deny his rights.
120. That UIDAI has provided stringent regulations for AUAs to ensure security of biometrics such as the mandate for Registered devices where Biometrics are sent encrypted from the device.

294

121. That it is submitted that UIDAI has a very robust security infrastructure and all necessary measures have been taken to ensure that the biometric information of the resident is secure. UIDAI has provided various measures to prevent misuse of biometric such as locking of biometric in CIDR, encryption of biometric data at all stages and use of PKI, 2048 bit encryption.
122. That in addition to the above, as per UIDAI circular dated 10.01.2018, Aadhaar number holders will have the option to generate Virtual ID (VID). VID is a temporary, revocable 16-digit random number mapped with the Aadhaar number. It is not possible to derive Aadhaar number from VID. There will be only one active and valid VID for an Aadhaar number at any given time. Aadhaar number holder can use VID in lieu of Aadhaar number whenever authentication or KYC services are performed. Authentication may be performed using VID in a manner similar to using Aadhaar number. VID is revocable and can be replaced by a new one by Aadhaar number holder. Therefore, resident would not need to share his/her Aadhaar number with anyone and still can authenticate using VID which can be changed anytime. VID is intended to add another layer of security to Aadhaar authentication system.
123. The contents of para 13 are incorrect and hence denied. UIDAI has taken several measures to ensure that tracking or profiling of

individuals is not possible. The foregoing paragraphs may be relied upon discussing the same.

124. Additionally UIDAI data is encrypted end to end and UIDAI databases are secured using a very robust encryption – PKI 2048 bit encryption. UIDAI logs do not have location or IP address details of the authentication device or location and hence tracking of individuals cannot be done.
125. Whenever authentication is done on UIDAI database, UIDAI receives minimal data for logging purposes. UIDAI does not get IP address of any system involved in the authentication chain.
126. The intermediate servers or telecom service provider or banking may store other details of the transaction as per the requirement of their parent Act. UIDAI have no control or access to these servers.
127. Therefore the location of authentication is not possible unless the UIDAI, government agencies, Internet service providers, AUAs/ASAs etc. together connives to breach all laws and contracts.
128. The allegations of the deponent are unfounded, incorrect and hence denied. As per the examples given by Mr. Kelekar use of credit card/Debit card should be banned as it can be used for locating / tracking as such information is available with banks. Cellular tower maintains locations of individuals, Internet/Mobile

applications/Mobiles/Laptops captures the IP address and GPS location. If such information is shared and government acts in unauthorized manner, internet too will become a tool for surveillance and social profiling.

129. **Allegations qua storage of biometric data by State Governments/Registrars**

130. The Petitioners have alleged that the Biometric Data which was collected at the time of enrollment by the Registrars prior to the enactment of the Aadhaar Act were being retained by the concerned State Governments/Registrars. After the provisions of the Aadhaar Act came into force with effect from 12.09.2016 and especially in light of Section 29(1) of the Aadhaar Act, 2016 it contained a clear prohibition against sharing of Biometrics with anyone for any reasons whatsoever and that it should only be used for the purpose of generation of Aadhaar and authentication under the Act. Therefore, in accordance with the above requirement of law, the UIDAI had issued a circular dated 17.04.2017 pursuant to its powers under Regulation 11 of the Aadhaar (sharing of information) Regulation, 2016 directing that the registrar packets, if any, available with the Registrars or any other agencies or their service providers authorized by the Registrar shall be destroyed by them in presence of a team of Officers from UIDAI not later than 30.04.2017. The Registrar shall also provide a certificate that they have destroyed the Registrar packet and that no Registrar Packet is available with them in the attached template. As per the circular

297

after the destruction, the Registrar shall handover the keys (private keys) of the Registrar Packet to the UIDAI team. In light of the above, it is submitted that most Registrars confirmed that they did not ever retain any biometric data and as for the rest, all State Government Registrars and State instrumentalities who were Registrars have destroyed biometric data in their servers which were collected during Aadhaar enrolment.

131. Illustratively, the Government of Maharashtra has issued a Certificate dated 23.06.2017 stating that no such Registrar Packets containing personal information of residents including sensitive Biometric information was found in the servers.

[A True Copy of the UIDAI Circular dated 17th April 2017 is attached herein and marked as Annexure R-27 at Pg. 333 to 334]

[A True Copy of the Certificate dated 23.06.2017 issued by the Government of Maharashtra is attached herein and marked as Annexure R-28 at Pg. 335 to].

132. The IDBI Bank vide its Letter dated 25.04.2017 has also confirmed that as a Registrar, it has not preserved any Resident Data as Registrar Packet including Biometrics and KYR+ of any Resident irrespective of whether it is a bank customer or not.

[A True Copy of the Letter dated 25.04.2017 issued by the IDBI Bank is attached herein and marked as Annexure R-29 at Pg. to 336]

298

133. A Certificate dated 28.04.2017 by Dena Bank certifies that Dena Bank is not holding any packets, particularly Biometrics, and other identity information collected as part of the process of Aadhaar Enrollment in its possession.

[A True Copy of the Certificate dated 28.04.2017 issued by Dena Bank is attached herein and marked as Annexure R-30 at Pg. to 337]

134. A Letter dated 27.04.2017 by the Jharkhand Agency for Promotion of Information Technology (JAP-IT) established under the Department of Information Technology, Government of Jharkhand states that pursuant to the UIDAI's Circular and as per Section 29(1) of the Aadhaar Act, the Registrar Packets with JAP-IT, kept on behalf of Department of IT, Government of Jharkhand has been destroyed in presence of a UIDAI team.

[A True Copy of the Letter dated 27.04.2017 issued by JAP-IT is attached herein and marked as Annexure R-31 at Pg. 338 to 339]

135. The Government of Himachal Pradesh has also issued a Certificate dated 09.05.2017 that all Registrar Packets have been destroyed and that no further Registrar Packet is available anywhere with the Registrar. It is also stated that the key for the Registrar Packet has been handed over to respective UIDAI Regional Office team.

[A True Copy of the Certificate dated 09.05.2017 by the Government of Himachal Pradesh is attached herein and marked as Annexure R-32 at Pg. 340 to 341.]

299

136. A Certificate dated 09.05.2017 by the Department of Food, Civil Supplies and Consumer Affairs, Punjab cum Registrar UID, Punjab has certified the destruction of available Registrar Packets and that no further Registrar Packets are available anywhere with the Registrar. The Keys to the Registrar Packet has also been handed over to the UIDAI Regional office team.

[A True Copy of the Certificate dated 09.05.2017 issued by Department of Food, Civil Supplies and Consumer Affairs, Punjab cum Registrar UID, Punjab is attached herein and marked as Annexure R-33 at Pg. 342 to 343]

137. The Letter dated 06.05.2017 issued by the State Bank of India certifies that no Registrar Packets are available with the State Bank of India for destruction.

[A True Copy of the Letter dated 06.05.2017 issued by the State Bank of India is attached herein and marked as Annexure R-34 at Pg. 344 to]

138. The Government of Rajasthan has issued a Certificate dated 19.04.2017 certifying that the State Registrar has destroyed all Registrar Packets along with Private Keys and that it is not holding any copy of such packets as well.

[A True Copy of the Certificate dated 19.04.2017 issued by the Government of Rajasthan is attached herein and marked as Annexure R-35 at Pg. to 345]

300

139. The Government of Goa has also issued a Certificate dated 04.05.2017 certifying the destruction of all Registrar Packet and that no further Registrar Packet is available anywhere with the Registrar.

[A True Copy of the Certificate dated 04.05.2017 issued by the Government of Goa is attached herein and marked as Annexure R-36 at Pg. 346 to 347]

140. The Collectorate, Daman as UIDAI Registrar has issued a Certificate dated 05.05.2017 certifying that no Registrar Packet is available with the Registrar and that the key for Registrar Packet has been handed over to the respective UIDAI regional office team.

[A True Copy of the Certificate dated 05.05.2017 issued by the Collectorate, Daman is attached herein and marked as Annexure R-37 at Pg. 348 to]

141. The Central Bank of India by its letter dated 30.05.2017 has confirmed that it does not have any Registrar Packet with it. Likewise, Bank of Baroda vide its Certificate dated 24.05.2017 has also confirmed that it is not holding any packets, particularly Biometrics and other identity information which were collected as part of Aadhaar Enrollment.

[A True Copy of the Letter dated 30.05.2017 issued by the Central Bank of India is attached herein and marked as Annexure R-38 at Pg. to 349]

301

A True Copy of the Letter dated 24.05.2017 issued by the Bank of Baroda is attached herein and marked as Annexure R-39 at Pg. to 350]

142. The Union Bank in its letter dated 26.05.2017 has confirmed that all the Registrar Packets have been destroyed in presence of the UIDAI Regional Office team and that no Registrar Packet is available with them.

[A True Copy of the Letter dated 26.05.2017 issued by the Union Bank is attached herein and marked as Annexure R-40 at Pg. to 351]

143. The Bank of Maharashtra vide Certificate dated 18.05.2017 has confirmed that it is not holding any Registrar Packet particularly Biometrics and other Identity information which were collected as part of Aadhaar Enrollment.

[A True Copy of the Certificate dated 18.05.2017 issued by the Bank of Maharashtra is attached as Annexure R-41 at Pg. to

352]

144. A Certificate dated 09.05.2017 by the NSDL E-Governance Infrastructure Limited certifies that it has destroyed all the Registrar Packets available and that no further Registrar Packet is available anywhere with the Registrar.

302

[A True Copy of the Certificate dated 09.05.2017 issued by NSDL E-Governance Infrastructure Limited is attached and marked herein as Annexure R-42 at Pg. to 353]

145. The Government of Gujarat by way of a Certificate dated 09.05.2017 has confirmed the destruction of all Registrar Packets and no Registrar Packet is available anywhere with the Registrar. Further the Key for the Registrar Packet has been destroyed.

[A True Copy of the Certificate dated 09.05.2017 issued by the Government of Gujarat is attached herein and marked as Annexure R-43 at Pg. to 354]

146. The Government of Tripura by way of Certificate dated 04.08.2017 has certified that they have destroyed all the Registrar Packets in presence of a team of UIDAI officials and that no Registrar Packets are available anywhere with the Registrar. Further, The Key for the Registrar Packet has also been handed over to the UIDAI Regional Office Team.

[A True Copy of the Certificate dated 04.08.2017 issued by the Government of Tripura is attached herein and marked as Annexure R-44 at Pg. to 355]

IV. ALLEGATIONS DEALING WITH INACCURATE CLAIMS QUA SAVINGS

147. It was alleged by the Petitioners that under MGNREGA - 67,637 job cards only were fake which could save only Rs.

303

127.88 Crores and therefore the estimated savings by the Government is inaccurate and exaggerated.

148. The allegation is denied is incorrect and based on a poor understanding of facts and economics.

149. **DBT UNDER MGNREGA**

a. Ministry of Rural Development has informed that under Mahatma Gandhi NREGA DBT is a major reform process where benefits are credited directly in to the bank accounts of MGNREGA workers, preferably Aadhaar Based Payments, cutting several layers in the delivery process. This helps in better targeting, increasing the efficiency of the system and reducing the delays in payments, ensuring greater inclusion, curbing leakage and thereby controlling expenditure and promoting greater accountability and transparency.

b. As of now, against the 11.2 crore active MGNREGA workers, the Aadhaar number of 9.9 crore (89%) active workers have been seeded into MGNREGA program database (NREGASoft) with the consent of the beneficiaries and 6.59 crore are enabled for Aadhaar based payments.

c. There are total 9.75 crore accounts of the MGNREGA active workers in Bank/ Post Offices. Of this, 9.01 crore (92%) accounts are in Banks and 0.74 crore (08%) accounts are in Post Offices.

150. Important measures taken by the Ministry that have helped sanitize the MGNREGS database are:

- a. Aadhaar camps organized at Block/ Gram Panchayat level in association with Banks for seeking consent for seeding.
 - b. Aadhaar number seeding in to the programme database (NREGASoft),
 - c. 96% of the total payments are done electronically directly into Bank/ Post Office accounts of the MGNREGS beneficiaries. Efforts are being taken to enable Aadhaar based payments for all active workers.
 - d. Extensive exercise has been carried out across all states/ UTs to verify all the MGNREGS job cards. This exercise also involves weeding out the duplicate/ fake job card. As of now there are 12.6 Crore Job card under MGNREGA. Since FY 16-17 (So far) out of the total 95% of the job cards verified 1.50 crore job cards have been deleted.
151. **DBT SAVINGS** - The DBT saving reported earlier were in terms of increasing the efficiency and reducing the delays in payments. Since the methodology was not firmed up the following was reported earlier:

	FY 2014-15	FY 2015-16	FY 2016-17
Basis of DBT calculation	12 Percent	15 percent	10 percent
Reported to DBT Mission (Rupees in Crore)	3000	4633	4108

- a. A study referred to in Economic Survey 2016-17, estimates an out-of-system leakages of 20% in MGNREGS Targeting (2011-12). In addition, sample data from Andhra Pradesh & Telangana and another study done in FY 14-15 in West Bengal,

305

reveal large variations in the number of bogus and ghost workers across the States ranging between 4% and 18%. They also indicate the potential savings if these irregularities are curbed.

- b. Recently Institute of Economic Growth, New Delhi, had conducted an independent study on quality of implementation of NRM component under MGNREGS. It has submitted the report to the Ministry on 5th January, 2018. This study report speaks of very good quality assets and general satisfaction of the beneficiaries with the way the programme is being implemented. This kind of perception of the beneficiaries indicates that there is plugging of loop holes in the overall architecture of the programme including payment of wages system.
- c. Based on the above, the DBT saving methodology has been firmed up by the Ministry and it is estimated that under MGNREGS on an average 10% of the expenditure on wages is being saved every year due to the above interventions.
- d. Owing to the sanitization of MGNREGA database by linking it to unique identity like Aadhaar the savings under the programme is as follows:

	FY 2017-2018 (So far)
Basis of DBT calculation	10 percent
DBT Saving as of 08 th Feb, 2018	3678
Wages expenditure (Rupees in Crore)	36,779

152. That the Petitioners have relied on the minutes of a meeting of the Committee of Secretaries held on 23.11.2015, wherein, it was observed that the annual LPG subsidy savings was Rs. 91 Crores. It is submitted that Petitioner's contention is denied since the basis of the Petitioner's calculation is incorrect, myopic and fails to take into consideration the ground realities. Further, the minutes have been quoted out of context and only capture the duplicates which were deleted from the database on being found out and not the ones who would have abandoned the subsidies on fear of being caught and neither does it account for the potential savings which would accrue to the government on account of large numbers of frauds and fakes who would be deterred from entering the system due to Aadhaar.
153. That the Ministry of Petroleum & Natural Gas *vide* its Office Memorandum No. P-20019/53/2014-LPG (P1) dated 9th February, 2018 has explained the method of calculation of savings in response to the Petitioner's submissions.
154. That during the implementation of PAHAL, intensive exercise was carried out for identifying duplicate/fake/ghost/inactive domestic LPG connections and, as of 01.04.2015, 3.34 Crore such connection were identified by the Oil Marketing Companies (OMCs). As a result of implementation of DBTL (PAHAL) mechanism, it became possible to block these 3.34 Crore LPG connections as the subsidy was transferred in the accounts of only those consumers who had registered under PAHAL and who have

307

been cleared after de-duplication exercise. Before DBTL, all or many of these 3.34 Crore consumers would have continued to purchase subsidized cylinders from the distributors. But for the blocking of these accounts, the subsidy bill would have been much higher despite the fall in crude oil prices.

155. It is submitted that the estimated savings from the aforementioned efforts can be calculated as follows:

- a. For the financial year(FY) 2014-15, for 3.34 crore consumers outside the PAHAL net, the estimated savings would be 3.34 Crores x 12 cylinders x Rs. 369.72 (average subsidy/cylinder for FY 2014-15) equal to Rs. 14,818.4 Crores. Following a similar principle, the savings estimated for FY 2015-16 is Rs. 6,443 Crore and FY 2016-17 is Rs. 4,608 Crore respectively.
- b. The total consumption of cooking gas in any given year is a combination of the number of connections at the beginning of the year, bogus connections eliminated during the year through the process of DBT under PAHAL, new connections issued to genuine consumers during the year and normal fluctuations in individual consumption. Hence, the saving from implementation of DBT cannot be correctly computed merely by reference to the total consumption in a year or the total expenditure on subsidy. If the DBT had not been implemented, the outgo on the subsidy would have been higher by Rs. 14,818 Crore in 2014-15, Rs. 6,443 Crore in 2015-16 and Rs. 4,608 Crores in 2016-17. This figure is not comparable with the actual expenditure on subsidy

368

which includes the subsidy on new genuine connections given during these three years. Without implementation of PAHAL, subsidy burden would have been higher than the actual expenditure recorded during these years, even with lower petroleum prices. That it must also be noted that concrete evidence of successful elimination of bogus connections is seen in the phenomenal growth of non-subsidized commercial LPG sales which have registered an increase of 39.3% in the period April, 2015 to March, 2016. This is in contrast to the pre-Pahal experience when commercial sales growth was negligible or declining.

156. That on a consideration of the aforementioned explanation by the Ministry of Petroleum and Natural Gas vis-à-vis the savings observed through the minutes of meetings of the Committee of Secretaries held on 23.11.2015, it is submitted that the Committee of Secretaries was only referring to the savings on account of duplicate connections which were blocked, as compared to the analysis by the MoPNG which has made a thorough analysis of the total savings that has resulted from PAHAL.

PUBLIC DISTRIBUTION SYSTEM (PDS)

157. That the Petitioners have questioned the Savings resulting from the Public Distribution System (PDS) as having resulted from DBT/Aadhaar based on answers furnished by the Minister of Consumer Affairs, Food and Public Distribution in the Lok Sabha.

309

158. That the contention of the Petitioner is denied for misconstruing the facts on record. As informed by Ministry of Consumer Affairs, Food and Public Distribution, on perusal of the answer provided by the Minister of Consumer Affairs, Food and Public Distribution in the Lok Sabha, it is clear that there is no contradiction in the claims by the Government about deletion of 2.33 Crore ration cards leading to a savings of Rs. 14,000 Crores per year and the statement furnished by the Minister of Consumer Affairs, Food & Public Distribution, Department of Food & Public Distribution during the reply to Lok Sabha for Unstarred Question No. 1517 dated 26th July, 2016. It has been clearly mentioned by the Hon'ble Minister that Cancellation of ration cards did not mean reduction in allocation or any savings in the budget expenditure for food subsidies, as the resulted savings were utilized for selection and provision of ration of new eligible beneficiaries under the NFSA by the concerned State Government.
159. That the averments made in the Additional Affidavit dated 16.02.2018 in W.P. (C) No. 829 of 2013 are denied as incorrect and contrary to the factual and legal position. It is denied that the Authority intends to carry out any biometrics experiment on anybody whatsoever, infants or otherwise. It is submitted that the Authority acts strictly within the purview of and under the aegis of the Aadhaar Act, 2016.
160. It is also denied that Biometric based authentication has excluded residents in Delhi or anywhere else from access to essential

310
14

services such as the PDS and the Petitioner has failed to consider that there is an exception handling mechanism in place, which is consistent with Section 7 and if there is any failure of authentication, benefits or subsidies cannot be denied under the exception handling mechanism which has been repeated in several circulars and instructions placed hereinbefore.

161. In view of the above submissions and reply to the additional facts raised by the Petitioners during oral arguments, the present Writ Petitions deserve to be dismissed.

162. That the Respondent herein reserves its right to file a further Affidavit if the Petitioners rely upon new facts which may require to be controverted or traversed in the interest of justice.

AND FOR THIS ACT OF KINDNESS, THE ANSWERING RESPONDENT AS IN DUTY BOUND SHALL EVER PRAY.

DEPONENT

VERIFICATION

I, the deponent named above do hereby verify that the facts stated in the above affidavit are true to my knowledge and belief, derived from the records of the case, nothing material has been concealed therefrom and no part of it is false.

Verified at on this 09th day of March, 2018.

DEPONENT

Drawn & Filed By:

Zoheb Hossain, Advocate

Dated: 09.03.2018

311
Annexure R-8

ITEM NO.9

COURT NO.2

SECTION XIV

S U P R E M E C O U R T O F I N D I A
R E C O R D O F P R O C E E D I N G S

SPECIAL LEAVE PETITION (CIVIL) Diary No(s).34292/2018

(Arising out of impugned final judgment and order dated 24-07-2018 in WP(C) No.7444/2018 passed by the High Court Of Delhi At New Delhi)

UNION OF INDIA & ORS.

Petitioner(s)

VERSUS

SHREYA SEN & ANR.

Respondent(s)

(FOR ADMISSION and I.R. and IA No.164367/2018-CONDONATION OF DELAY IN FILING SLP and IA No.164370/2018-EXEMPTION FROM FILING C/C OF THE IMPUGNED JUDGMENT and IA No.164368/2018-CONDONATION OF DELAY IN REFILING SLP)

Date : 04-02-2019 This petition was called on for hearing today.

CORAM :

HON'BLE MR. JUSTICE A.K. SIKRI
HON'BLE MR. JUSTICE S. ABDUL NAZEER

For Petitioner(s) Mr. K. K. Venugopal, Ld. AG
Mr. Zoheb Hossain, Adv.
Mr. Rupesh Kumar, Adv.
Mrs. Shradha Deshmukh, Adv.
Mrs. Anil Katiyar, AOR

For Respondent(s) Mr. Mohit Chaudhary, AOR
Ms. Puja Sharma, Adv.
Mr. Balwinder Singh Suri, Adv.
Ms. Tripty Poddar, Adv.

UPON hearing the counsel the Court made the following
O R D E R

Delay condoned.

The High Court *vide* impugned order dated 24.2.2018 passed in

Signature Not Verified
Digitally signed by
SANJAY KUMAR
Date: 2019.02.05
16:59:05 IST
Reason:

Petition (Civil) No.7444 of 2018, had permitted the Respondents herein to file the Income Tax Return for the Assessment Year 2018-19 without linkage of their Aadhar and PAN numbers and it was also directed that the Income Tax Department would not insist

312✓

on production of their number of Aadhar enrolment.

The aforesaid order was passed by the High Court having regard to the fact that the matter was pending consideration in this Court. Thereafter, this Court has decided the matter and upheld the vires of section 139AA of the Income Tax Act. In view thereof, linkage of PAN with Aadhar is mandatory.

Insofar as assessment year 2018-19 is concerned, learned counsel appearing for the respondents informs that the respondents had filed the income tax returns in terms of the orders of the High Court and the assessment has also been completed.

We therefore make it clear that for the assessment year 2019-20, the income tax return shall be filed in terms of the judgment passed by this Court.

The special leave petition is disposed of in the above terms.

Pending interlocutory applications, if any, stand disposed of.

(SANJAY KUMAR-II)
COURT MASTER (SH)

(SANTOSH KUMAR)
COURT MASTER (NSH)

3/3

Annexure R-9

PRIME MINISTER'S OFFICE

South Block, New Delhi - 110 011

Please find enclosed a copy of Records of Discussion of the meeting chaired by the Principal Secretary to PM on "Aadhar Enrolment in Post Offices and Bank Branch Premises" on 29.09.2017 at 04.00 PM, Prime Minister's Office, South Block, New Delhi, for further necessary action.


(Brijesh Pandey)
Deputy Secretary
Tel. 23013586

Finance Secretary
Secretary, D/o Financial Services
Secretary, M/o Electronics & Information Technology
Secretary, D/o Posts
CEO, UIDAI
PMO ID No: 460/32/C/14/2017-ES.1

Dated: 06.10.2017

314

923

RoD of the meeting taken by the taken by the Principal Secretary to PM on 'Aadhaar Enrolment in Post Offices and Bank Branch Premises.

Date: 29.09.2017

Venue: PMO, South Block

Time: 04.00 p.m.

List of the participants is Annexed.

2. The main points of discussion and the decisions taken in the meeting are as under:

(i) UIDAI to phase out all private agencies for enrolment and updation of Aadhaar by the end of December, 2017. Thereafter, only Bank Branches and Post Offices will be locations for Aadhaar enrolment and updation.

(Action by: UIDAI)

(ii) UIDAI may also have consultation with the States as they might have outsourced work of Aadhaar enrolment. The effort should be to phase out outside agencies without causing inconvenience to the general public in enrolment and updation.

(Action by: UIDAI)

(iii) UIDAI to send monthly progress reports on phasing out outside private agencies in enrolment and updation.

(Action by: UIDAI)

(iv) D/o Posts has opened 803 update centres till date. They will be opening a total of 14,200 Aadhaar enrolment centres by December, 2017. The centers shall be operated by Department of Posts directly without involvement of any private Aadhaar enrolment agencies. The monthly target for opening centres should be fixed for next 3-months.

(Action by: D/o Posts)

(v) Rs.200 Crores will be released under Demand No.32 of NITI Aayog immediately. The proposal to be submitted by UIDAI and D/o Posts.

(Action by: UIDAI / DoP / DOE)

(vi) Banks shall complete the task of setting up Aadhaar enrolment and update centers in 15,200 Bank Branches by Oct 31,

315

2017. The centers shall be operated by banks directly inside bank branches without involvement of any private Aadhaar enrolment agencies.
(Action by: DFS/UIDAI)

(vi) The existing authentication devices for Aadhaar authentication should be replaced with registered devices by user agencies including banks in a time-bound manner.
(Action by: UIDAI/DFS)

(vii) The consolidated kit for enrolment and updation should be made available on the GEM platform. Issues on this matter should be resolved by MeitY to ensure that kits are available on the GEM platform.
(Action by: MeitY)

(viii) UIDAI, in consultation with the D/o Posts, may revise the reimbursement charges for enrolment and updation at Post Offices. DoE to work out the modalities for reimbursing this expenditure to UIDAI/DOP.
(Action by: UIDAI / DoP / DoE)

The meeting ended with a vote of thanks to the chair.

Annexure

List of participants:

- 1 Shri A.N. Nanda, Secretary, D/o Posts
- 2 Shri Ajay Sawhney, Secretary, MeitY
- 3 Dr. Ajay Bhushan Pandey, CEO, UIDAI
- 4 Shri Rajiv Kumar, Secretary, D/o Financial Services
- 5 Shri Pramod Kumar Das, Addl. Secretary, D/o Expenditure
- 6 Smt Usha Chandrasekhar, Member(Operations), Department of Posts

From PMO:

1. Shri Tarun Bajaj, Addl. Secretary
2. Shri Anurag Jain, Joint Secretary
3. Shri Brajendra Navnit, Joint Secretary
4. Shri Brijesh Pandey, Deputy Secretary

REGD. NO. D. L. 33004/99

316
REGD. NO. D. L. 33004/99

Annexure R-10

भारत का राजपत्र The Gazette of India

असाधारण

EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (I)

PART II—Section 3—Sub-section (I)

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

नं. 8061

No. 8061

नई दिल्ली, सोमवार, दिसम्बर 21, 2015/अग्रहायणा 30, 1937

NEW DELHI, MONDAY, DECEMBER 21, 2015/AGRAHAYANA 30, 1937

संचार एवं सूचना प्रौद्योगिकी मंत्रालय

(इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग)

(भारतीय विशिष्ट पहचान प्राधिकरण)

अधिसूचना

नई दिल्ली, 11 दिसम्बर, 2015

सा. का. नि. 993(अ).—सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21*) के अनुच्छेद 70 के उप-अनुच्छेद (1) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, केंद्र सरकार, एतद्वारा घोषित करती है कि यू.आई.डी.ए.आई. की केंद्रीय पहचान डेटा भंडार (सी.आई.डी.आर.) सुविधाएं, इसका हार्डवेयर और सॉफ्टवेयर, सूचना परिसम्पत्तियां, लॉजिस्टिक अवसंरचना और डिपेंडेंसिज आदि जो कि यू.आई.डी.ए.आई. (भारतीय विशिष्ट पहचान प्राधिकरण) के लोकेशन पर संस्थापित हैं—उन्हें सूचना प्रौद्योगिकी अधिनियम 2000 के उद्देश्य से संरक्षित सिस्टम माना जाएगा।

आई.सी. एक्ट 2000 (संशोधित 2008) के अनुच्छेद 70 के उप-अनुच्छेद-2 के अनुसार प्राधिकृत कार्मिकों, जिनके पास कार्य आधारित पहुंच होगी, केवल उन्हीं को ही यू.आई.डी.ए.आई.-सी.आई.डी.आर. सुविधाओं तक जाने का अधिकार होगा:

1. यू.आई.डी.ए.आई. के पदनामित अधिकारी और स्टाफ।
2. मैनेज्ड सर्विस प्रोवाइडर (एम.एस.पी.) के अनुबंधित सदस्य, जिन्हें यू.आई.डी.ए.आई. ने प्राधिकृत कर रखा हो।
3. अन्य प्राधिकृत थर्ड पार्टी वैंडर्स और इनके पार्टनर्स।
4. यू.आई.डी.ए.आई. के विजिनेस पार्टनर्स।

[सा. स. डी-10(36)/2015-ईजी-II],

राजीव कुमार, संयुक्त सचिव,

5348 GI 2015

(1)

312

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

(Department of Electronic and Information Technology)

(UNIQUE IDENTIFICATION AUTHORITY OF INDIA)

NOTIFICATION

New Delhi, the 11th December, 2015

G.S.R. 993(E).— In exercise of the powers conferred by sub-section (1) of Section 70 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby declares the UIDAI's Central Identities Data Repository (CIDR) facilities, Information Assets, Logistics Infrastructure and Dependencies Installed at UIDAI (Unique Identification Authority of India) locations to be Protected System for the Purpose of Information Technology Act 2000.

Authorised personnel as per Sub-section (2) of Section 70 of IT Act 2000 (amended 2008) having role based access to UIDAI-CIDR facility are:

1. Designated UIDAI officers & Support Staff.
2. UIDAI authorised team members of contracted Managed Service Provider (MSP).
3. Other authorised third party Vendors and its partners.
4. UIDAI authorised business partners.

[F. No. 10(36)/2015-EG-III]

RAJIV KUMAR, Jt. Secy.

31.8
Annexure R-1114th September, 2017

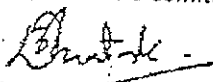
Report of the Committee to undertake Outcome Review of the UID Scheme

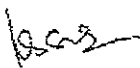
A Committee comprising of following members was constituted to undertake Outcome Review of UID Scheme -

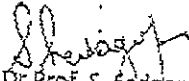
(i) Dr. Prof. Deepak B. Phatak, Dept. of CSE, IIT Mumbai	---	Chairperson
(ii) Dr Prof. Rajat Moona, Director, IIT Bhilai	---	Member
(iii) Dr Prof. S. Sadagopan, Director, IIT Bangalore	---	Member

Smt. Deepali Sharma, ADG, UIDAI was deputed as the convener of the Committee.

2. The Committee was constituted as per the directives of the Ministry of Finance's OM Nos. 42(02)/PF-II/2014 dated 23.02.2017 and 27.03.2017 (copies enclosed), in which, the scheme owner Ministries are directed to undertake an outcome review of their schemes at the end of 12th Five Year Plan (March 2017) and submit the same for appraisal & approval of Expenditure Finance Committee (EFC) for continuation beyond 12th Plan to make them co-terminus with the 14th Finance Commission Period or beyond.
3. The Terms of Reference (ToR) of the Committee are to;
 - (i) Carryout an outcome review of UID scheme.
 - (ii) Evaluate whether the scheme is effective in delivering its objectives and whether there is a need for continuation of the scheme in view of its mandate and performance.
 - (iii) Ascertain whether the scheme can continue in its present form and suggest changes, if needed.
 - (iv) Any other suggestion.
4. The Committee met on 28.08.2017 at Indian Institute of Technology, Mumbai and then on 14.09.2017 at UIDAI Technology Center, Bangalore to discuss the overall objectives of UID Scheme, performance and achievements of UIDAI till March 2017, and future plans of UIDAI.
5. The report of the Committee is attached herewith.


Dr. Prof. Deepak B. Phatak
(Dept. of CSE, IIT Mumbai)


Dr Prof. Rajat Moona
(Director, IIT Bhilai)


Dr Prof. S. Sadagopan
(Director, IIT Bangalore)

Report of the committee

On

The Outcome Review of the UID Scheme

Submitted by

Prof. Rajat Moona, Director, IIT Bhilai

Prof. S. Sadagopan, Director, IIIT Bangalore

Prof. Deepak B. Phatak, Dept. of CSE, IIT Bombay

Submitted on

14 September 2017

Contents

Executive Summary	iii
1. Preamble	1
2. Approach and Methodology adopted by the Committee	2
3. Detailed report	3
4. Suggestions and Recommendations of the Committee	8
5. Acknowledgments	10
Annexures:	
Annexure 1- Aadhaar Act, 2016	11
Annexure 2- Synopsis of EFC approvals and Expenditures with Revised Cost Estimates	13
Annexure 3 (A)-Overall achievements of Aadhaar	15
Annexure 3 (B) - UID as a Net Positive Scheme	16
Annexure 4- Data Security and Privacy	19
Annexure 5- Security of data in CIDR	21
Annexure 6- Data Security in collection/use of Aadhaar data	23
Annexure 7 - New Security initiatives by UIDAI	25
Annexure 8 - Justification for Continuation of scheme	27

Report of the committee on the outcome review of the UID scheme
[Summary for executive perusal]

321

1. A committee was constituted on 21 August 2017, to undertake the outcome review of the Unique Identification Scheme (UID), comprising Prof. Rajat Moona, Prof. S. Sadagopan, and Prof. Deepak B. Phatak (Chairman).
2. Committee first collected the necessary background information from UIDAI. Two meetings were held. In each of these, UIDAI officials were requested to make detailed presentations on all aspects of the scheme. Clarifications were sought where needed, which were duly provided. During one of the meetings, the committee visited the Data Centre in Bengaluru. The visit was primarily to ascertain that the large server and storage farms have been installed with a world class infrastructure. An additional objective was to appraise first-hand, the data security measures being implemented.
3. After extensive examination of all facets, the committee has prepared its report. Main observations and recommendations of the committee, with respect to specific ToRs (Terms of Reference), are summarized below:

ToR 1: Committee has carried out a detailed review of the outcome of the UID scheme, and notes that the objectives have been fully achieved, and further, have been surpassed.

ToR 2: Committee finds that the Scheme has been successful in delivering its objectives. Committee notes that critical 'identity authentication' service is provided by the scheme. This is being used by various Government and Non-Government Services like Subsidy Benefits, Pensions, Scholarships, Social Benefits, Banking, Insurance, Taxation, Education, Employment, Healthcare, etc. It is necessary to cover the number of newborn Indians (About 2 Crore per year), as also to capture the biometric updates at the age of 5 and 15. The committee is of the opinion that the scheme, in fact, must run in perpetuity. Committee strongly recommends continuation of the scheme, with adequate financial support.

ToR 3: Committee recommends that the scheme can and should run in its present form.

ToR 4: Committee has made several recommendations to enhance the efficacy and effectiveness of the scheme. Committee notes with satisfaction that enhanced security measures have been undertaken. It recommends that these be speedily implemented.
4. Committee wishes to put on record that the concerned officials of UIDAI tirelessly worked to provide all the information required by the committee.

--- o o o ---

14 September 2017

Report of the Committee on the Outcome Review of the UID Scheme

322

1. Preamble

UIDAI was established in the year 2009, as an attached office of the then Planning Commission (now NITI Aayog), vide its Gazette Notification No.A-43011/02/2009-Admn.I dated 28 January 2009. Subsequently, the Government revised the Allocation of Business Rules on 12 September 2015, to attach UIDAI to the then Department of Electronics & Information Technology (DeitY), Ministry of Communications and Information Technology, now Ministry of Electronics & Information Technology (MeitY). As on today, the Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of Aadhaar Act, 2016, under the Ministry of Electronics and Information Technology (MeitY).

A Committee comprising the following members was constituted to undertake Outcome Review of UID Scheme -

(i) Prof. Deepak B. Phatak, Dept. of CSE, IIT Mumbai	Chairperson
(ii) Prof. Rajat Moona, Director, IIT Bhilai	Member
(iii) Prof. S. Sadagopan, Director, IIT Bangalore	Member

Smt. Deepali Sharma, ADG, UIDAI, was deputed as the convener of the Committee.

The Committee was constituted as per the directives of the Ministry of Finance's OM Nos. 42(02)/PF-II/2014 dated 23.02.2017 and 27.03.2017 (copies enclosed), in which the scheme owner Ministries are directed to undertake an outcome review of their schemes at the end of 12th Five Year Plan (March 2017), and submit the same for appraisal and approval of Expenditure Finance Committee (EFC) for continuation beyond 12th Plan, to make them co-terminus with the 14th Finance Commission Period or beyond.

The Terms of Reference (ToR) of the Committee were:

- (i) Carry out an outcome review of UID scheme.
- (ii) Evaluate whether the scheme is effective in delivering its objectives, and whether there is a need for continuation of the scheme in view of its mandate and performance.
- (iii) Ascertain whether the scheme can continue in its present form, and suggest changes if needed.
- (iv) Make any other suggestion.

This report provides the detailed findings of the committee, and its recommendations.

2. Approach and Methodology adopted by the committee

Members of the committee were generally familiar with the work that has been done so far by the UIDAI, as also its widespread use by several other schemes and programs. However, a critical assessment of the outcomes necessitated a very detailed analysis of the progress made, as also to understand how the scheme will benefit in future years, if recommended for continuation.

In view of the above, the committee decided to adopt the following approach:

1. UIDAI was requested to provide detailed background information, along with supporting documents.

2. Members studied this material, raised queries where needed, and sought clarifications. All members were kept informed of such clarifications.
3. The Committee conducted its first meeting on 28.08.2017 at Indian Institute of Technology Bombay, Mumbai. In this meeting, UIDAI officials were requested to make brief presentations on the achievements of the scheme, and proposed activities in case the scheme is continued.
4. Members then discussed these inputs over next several days. It was felt that a visit to the main Data Centre should be undertaken, to ensure that the infrastructure is well established as per global norms, and also to obtain a first-hand understanding of the data security measures implemented by UIDAI.
5. The second and final meeting of the committee, was held in Bengaluru on 14 September 2017. Members visited the Data Centre. Detailed explanation was provided by the Data Centre team about the basic infrastructure, and how it meets the global standards. Committee was informed that the second Data Centre in Manesar has been so planned as to meet the requirement of having two facilities in two different seismic zones.
6. Specific inputs were sought by the committee regarding the data security measures incorporated. Presentations were made by the concerned team leaders, explaining the measures which have already been put in place. Members pointed out that data security needs to be enhanced on a continuous basis. A detailed presentation was made on the continuous efforts being taken in this regard.

The committee prepared this final report at the conclusion of the second meeting. Details, wherever required, have been provided by the UIDAI officials. After confirming the correctness of the information as per records, the committee has included the relevant details in appropriate annexures.

3. Detailed report

Section 23 of the Aadhaar Act outlines the powers and functions of the Authority, as presented in Annexure 1.

A detailed document on Establishment of UIDAI by executive order, mandate of UIDAI, fund approvals for UID Scheme by the government in 5 phases, performance of scheme against the targets and other areas, figures showing UID as a net positive Scheme, and justification for continuation of the Scheme, was shared with the committee members. A presentation on the same was also given to the Committee by UIDAI, in the first meeting held at IIT, Mumbai. As desired, by the committee, in the first meeting, detailed notes on data security and privacy safeguards taken by UIDAI, and Aadhaar grievance redressal mechanism, were shared with the Committee before second meeting. During the second meeting, detailed presentations on data security and privacy safeguards in UIDAI and various new data security initiatives, like Secure Aadhaar Enrolment system, Aadhaar virtual ID, and Registered Devices, were made to the Committee, followed by a visit to the Data Center, Bangalore.

The committee deliberated on performance and achievements of UIDAI, during these meetings, and held detailed discussions on the technology architecture, information security systems, and legal framework adopted by UIDAI for ensuring data security and privacy of Aadhaar holders.

324

The brief of the discussions and conclusions of the committee in both meetings, are given below:

1. UIDAI has been allocated funds in five sets of financial installments, for the establishment of UIDAI, and fulfilling its mandate. Approvals totaling Rs 13,663.22 crore have been granted to UIDAI in five (5) phases, and Revised Cost Estimate (RCE) of Rs 150.26 crore was subsequently sanctioned by the Competent Authority as per Department of Expenditure, Ministry of Finance O.M. No. 24(35)/PF-II/2012 dated 29.08.2014 and 05 August 2016, making the total scheme fund approval to total Rs 13813.48 crore. A statement showing component-wise EFC approvals in five phases, and the expenditure incurred up to March 2017, as presented to the committee, is given in Annexure 2.
2. The committee noted that the achievements of UIDAI have been far beyond the targets given. UIDAI was allocated Rs.13,663.22 crore to cover enrolment of 91.62 crore residents against which UIDAI has generated 113.28 crore Aadhaar numbers by March 2017, within a total expenditure of Rs 8793.86 crore. This brings per unit cost of issuing Aadhaar, to Rs 77.62 only, which includes expenditure on 2.54 crore updates, 554.17 crore authentication, and 117.01 crore e-KYC transactions.
3. The Committee acknowledged that UIDAI is the largest biometric based unique identity system, which is unparalleled in the world. The committee noted that UIDAI has overall achieved its given target, and in fact has surpassed it. UID scheme has rendered direct economic benefits to the tune of Rs 57,030 crore by the end of FY 2016-17 to the government, as captured by DBT Mission. Overall achievements of Aadhaar are presented in brief in Annexure 3 (A). In addition, Aadhaar linkage has benefitted the government and Aadhaar holders, in many other ways, as presented in Annexure 3 (B) which clearly outlines it as a net positive scheme.
4. UIDAI commenced Aadhaar generation in 2010 from a hired Data Centre (DC) in Bangalore. Subsequently, Disaster Recovery (DR) Data Centre was hired in 2011 in Greater Noida. UIDAI managed its operations from the two hired Data Centers till 2015 wherein, approx. 90 crore Aadhaar were generated, and a number of services like update, authentication, eKYC, etc were launched. UIDAI's own DC and non DC buildings were completed in 2015 and UIDAI migrated its operations from hired DC to Hebbal (Bangalore) DC, in December 2015, and to Manesar DC, in June 2016, without any interruption in services.
5. The committee reviewed the Aadhaar enrolment status in states and UTs, and appreciated the overall progress. The committee suggested UIDAI to focus on covering left out population in states where more than 1 crore population is remaining, in particular, in the 0-5 years and 5-18 years age group. The committee advised UIDAI to focus more on providing Aadhaar Authentication, Updation services, and grievance handling.
6. The committee appreciated progress on proliferation of Aadhaar authentication services through its 27 Authentication Service Agencies, 326 Authentication User Agencies, and 255 eKYC User Agencies, which have facilitated processing of over 865.05 crore authentication and 246.96 crore e-KYC requests by 15 Aug 2017. UIDAI is processing 2.6 crore authentications requests per day on a monthly average basis, with peak loads at 6 crore transactions per day. The Committee advised UIDAI to prepare for increase in authentication load, in phases. In the first phase, the Committee suggested to enhance the existing authentication transaction capacity of 10 crore per day to 40 crore/day in the coming three months, and to 120 crore/day in a period of next 10 months.
7. The committee was informed that UIDAI communicates Aadhaar number and demographic details to the residents through Aadhaar letter. UIDAI uses Ordinary

325

mail services of India Post, and till March 2017, UIDAI had printed 114.5 Crore Aadhaar letters (this includes 4.11 Crore letters sent by Speed Post in the initial days).

8. The committee was apprised of Grievance handling system of UIDAI, wherein on an average 1.5 lakh- 2 lakh calls and 2,500-3,000 emails are handled per day.
9. The committee acknowledged that Aadhaar is an important tool for the Government to achieve clean and good governance. This is evident from the fact that Aadhaar is required as an identity document by over 220 schemes, notified through over 137 notifications, by over 37 Ministries/Departments, as on 15th August 2017. Also, Aadhaar is increasingly being used by the government to transfer cash benefits directly to the beneficiaries' accounts as evident from the transaction volumes, wherein over Rs. 62,635 crore have been paid across 228.04 crore successful transactions, by 15th August 2017.
10. The committee acknowledged that Aadhaar is gaining popularity among the masses for doing financial transactions, in line with the goals of the Government and Reserve Banks of India for promoting financial inclusion and digital payments. New Aadhaar based payment systems like Aadhaar Payment Bridge (APB), Aadhaar Enabled Payment System (AEPS), Aadhaar Pay, and Pay to Aadhaar, have achieved critical volumes, and are driven now by users. Meanwhile, banks have been working extensively to empower Aadhaar holders by enabling Aadhaar Pay and Pay to Aadhaar in their systems and increasing presence of Aadhaar enabled devices in the field.
11. Physical Security- UIDAI informed that Security of Aadhaar data is paramount to UIDAI, and the Authority has taken several steps to ensure the same. UIDAI's CIDR facilities, information Assets, Logistics Infrastructure and Dependencies installed at UIDAI locations, have been declared as Protected System, to accord highest security. The Committee members praised the security features and upkeep of Data Centre, during the visit. The committee acknowledged the elaborate physical security systems put in place, like manning by armed CISF men, entry restrictions, access through biometrics devices, and monitoring of the complete area by motion sensitive cameras connected to the Building Management System Unit. Further, UIDAI ensures data security through three concurrent aspects viz technology design, processes, and law.
12. Data protection and privacy by design- Aadhaar is designed on the principles of Minimal Data, Optimal Ignorance, and Federated Database, which will prevent UIDAI, Government or for that matter any Department or Agency, to track and profile any individual. Minimum data is collected by UIDAI which is used only for Aadhaar generation and providing Authentication services. UIDAI, while providing identity Authentication service, only informs the requesting agency whether the particular Aadhaar number and provided biometric is matching or not matching. UIDAI only knows that a resident's identity is authenticated by a particular agency at a particular time, as it never asks for the purpose and location of transaction, and hence, no profiling of the person is possible. The Demographic and core Biometric data is stored in different databases and is uniquely identified through Reference ID (federated database structure). Besides, Aadhaar database is not linked with any other Govt/State/Private information system.
13. Sharing of Data- As per Section 29 and 33 of Aadhaar Act, no Aadhaar data (Aadhaar number and demographic details), can be shared by any individual or entity, with any individual or entity, without the consent of the resident, for that particular purpose. The shared data can be used for that particular purpose only. Similarly, the Aadhaar number of an individual shall not be published, displayed, or posted

326

- publicly by any person, or entity, or agency. Biometric details can never be shared with anyone even with the consent of the individuals, except in case of National Security with the approval of a Committee headed by the Cabinet Secretary.
14. Data Security and Privacy safeguarded by law- Aadhaar Act, 2016, has ensured that all technological and organizational measures are in place to ensure the confidentiality and privacy of resident data. Specific provisions in the Act, ensuring security of data, are presented in Annexure 4. The Aadhaar Act 2016 (Chapters VI & VII) read together with Aadhaar (Data Security) Regulations, 2016 (No. 4 of 2016) pursuant to clause (p) of sub-section 2 of section 54 of the Aadhaar Act 2016, and Aadhaar (Sharing of Information) Regulations, 2016 (No. 5 of 2016) pursuant to sub section 1 and sub clause (o) of sub section (2) of Section 54, read with sub clause (k) of sub section (2) of section 23, and sub sections (2) & (4) of Section 29 of the Aadhaar Act 2016, provides several safeguards in the form of security and confidentiality of information, restrictions on sharing information, disclosure of certain information, and offences and penalties for breach of the Act or regulations.
 15. Data Security by Technology Infrastructure- Committee was informed that UIDAI has put in best practices and technology such as firewalls, Intrusion Prevention Systems, zoning and access control, centralized security policy management, audits, and 24x7 monitoring through Security Operations Centre (SOC) and Network Operation Centre (NOC). UIDAI is ISO 27001: 2013 standard compliant, that defines security protocols and access protocols to ensure the safety of data. The steps taken to ensure data security in CIDR, are presented in Annexure 5.
 16. UIDAI has also put in place, a comprehensive framework for protection and security of residents' data, and ensuring maximum accountability and transparency in the entire process of collection and use of data. The details of security provisioned in enrolment and use of Aadhaar (authentication system) are presented in Annexure 6.
 17. Biometric locking- UIDAI provides biometric lock facility to all the Aadhaar number holders using which Aadhaar number holders may lock their biometrics and may unlock when required. Residents can conveniently lock/unlock their biometrics using web services or mobile m-aadhaar application.
 18. UIDAI is working on other security features like Registered Biometric Devices wherein each biometric device will be uniquely identifiable, traceable, and biometric captured by this device will be encrypted at source; Issuing virtual ID and Aadhaar tokens and secure USB based ECMP client, detailed further in Annexure 7.
 19. UIDAI informed the committee that it continuously keeps scanning the environment and assessing need for new additional security initiatives. A couple of such initiatives mentioned below, were briefed to the committee, which are presented in Annexure 7.
 20. The nine judge bench of the Hon'ble Supreme Court in the matter whether the Right to Privacy is a Fundamental Right, has not commented on the Aadhaar Act or the usage of Aadhaar in any other law. Therefore, the usage of Aadhaar will continue to be governed by the provisions of the Aadhaar Act. Validity of Aadhaar Act will now be heard before the three judge bench of the Hon'ble Supreme Court before which Government will present its case of Aadhaar Act being fully compliant on the touchstone of Privacy as Fundamental Right as per the verdict of the Nine Judge Bench.
 21. UID as a net positive scheme- The good performance and success of UID scheme, is a well known fact. It was very informative and eye opening to know the performance and achievements of the project, in detail. Overall, the Committee is satisfied by the performance of UIDAI, and it clearly emerges as a net positive scheme (details in Annexure 3). Given the scale of the project, touching lives of all

327

Indian residents, and the fact that it is the largest biometric project in the world, the progress of the project is commendable. Touching more than 117 crore people in a span of 8 years, is a great feat for the UIDAI team, and that too at a cost of less than Rs 80 per Aadhaar, including all the services that have been rendered till date.

22. Justification for continuation of scheme- The Committee concurs with the proposal of UIDAI that, work of UIDAI on giving Aadhaar numbers to the residents of India, and offering Aadhaar updation and authentication services, is a work in perpetuity. UIDAI needs to continue its operations for providing Aadhaar numbers to new-born, provide updation services for all, including mandatory updates for children at the age of 5 years and 15 years, provide authentication services, and provide Aadhaar related services for financial inclusion and banking. In addition, the scheme needs to continue to act as a tool for good governance, and facilitate direct benefit transfer to the intended beneficiaries, so that it could further prevent leakages and save money (details in Annexure 8). Further, Aadhaar Act was passed and UIDAI was notified as an Authority, on 12 July 2016. The UIDAI has been given responsibilities under the Act to carry out these essential activities, and is a work in perpetuity.

4. Suggestions and recommendations of the Committee

With the above details, it is clear that the UID scheme has offered many economic and social benefits to the country, and clearly emerges as a NET POSITIVE scheme, and hence has full justifications to be continued. The committee has some suggestions for UIDAI to consider in its future plans:

1. The committee feels that technology infrastructure upgradation with time, is the most important thing for UIDAI. The committee observed that the IT infrastructure at CIDR may need replacement after it has lived its life, and increased usage will require more processing and storage capacity. Hence, UIDAI must consciously and strategically plan to maintain inventory of active in-service equipment of latest technology.
2. UIDAI must immediately focus on enhancing its Authentication capacity. UIDAI informed the Committee members that, it is processing a RFP to enhance authentication capacity of UIDAI to 40 Crore authentications per day. The committee feels that UIDAI must very shortly prepare to enhance it to nearly 120 crore per day.
3. About Aadhaar enrolments, the committee believes that it is time for UIDAI to focus on providing Authentication services and updation of Aadhaar, besides Aadhaar enrolment.
4. The committee finds a need to strengthen the grievance handling mechanism, and suggested that UIDAI should set benchmarks on grievance resolution timelines, and build escalation matrix. Considering the fast changing requirements of Aadhaar and its increased footprint, Aadhaar grievance handling mechanism will gain importance, and hence UIDAI should move towards new automated systems like AI based systems, chat bots, etc for grievance handling.
5. The committee observed that although UIDAI has put elaborate security system in place, there is a need to continuously strengthen it in view of new threats. The committee also observed that entities that are collecting Aadhaar or doing Aadhaar Authentication are to be made more secure. Their issues gets reported as UIDAI issues, and hence there is a need for awareness campaign on two aspects firstly, making the agencies aware of the security requirements of UIDAI, to avoid such breaches, and secondly, informing the general public about the responsibility of Aadhaar agencies, on security of their data.

3. Acknowledgments

The committee wishes to put on record, its sincere appreciation for the timely inputs provided by the UIDAI officials. These details were consolidated and shared with the members in the shortest possible time. Whenever any clarification was sought by any member, the same was provided immediately. Many senior officers personally participated in both the meetings. The committee appreciates this support, including the commitment shown by the senior leadership UIDAI. Committee could not have completed this exhaustive review, without such excellent support.

Chairman would like to record his personal appreciation to both members of the committee. They are loaded with work, as leaders of two of the leading National Institutions. They are also busy with several other commitments, which come their way due to their expertise and extensive experience. In spite of their tight schedule, they found and spent quality time for this important task, and attended meetings on dates which were imposed on them. Their contribution is gratefully acknowledged.

- 329
6. The Committee appreciated UIDAI's initiative and consciousness towards privacy at every step, by narrowly tailoring the provisions of the law, and ensuring that there is informed consent, and purpose limitation, as far as sensitive personal information is concerned. The committee feels that though UIDAI systems, processes and structure are carefully designed and applied, these are not publicized widely, giving opportunity to the critics to spread misinformation and create misconceptions about Aadhaar. Hence, UIDAI should proactively engage in awareness campaign on UIDAI security systems.
 7. Aadhaar number sharing and seeding in many databases can potentially create data linking issues. Committee appreciated the work UIDAI has begun for tokenization and virtualization of the ID to address this issue. Committee is in full support of this effort and suggests implementing it quickly.
 8. The Committee feels that third party authentication failure and the related denial of services (not releasing ration, for example) is the sole responsibility of the User Departments and not of UIDAI.
 9. The committee observed that UIDAI is dependent on Government for its finances, and its revenue is deposited in CFI. The UIDAI may consider becoming financially self sufficient. Presently, every year UIDAI requests the Government for appropriate budgetary support. It has been observed that budgetary support has been drastically reduced during the last two years. This will seriously impact functioning of UIDAI in short as well as long run.

Therefore, quantum of budgetary support had to be determined on a rational basis. For every service, appropriate cost may be determined by the Authority following a transparent and objective process, and this should be recoverable from the users of the service. If the Government wants to subsidize any of the services, may provide appropriate subsidy through budgetary support, and to that extent lesser charges may be recovered from the users. This is a standard process followed in the other regulatory sectors such as Electric supply where tariffs are reduced by subsidies. If budgetary support is determined in this manner, UIDAI can not only be self sufficient, but also be held accountable by users as well as the government. Based on the above, appropriate amendments in Aadhaar Act may be carried out accordingly.

Overall, the committee believes that the project has helped in giving a dignified life to individuals. Considering the strong de-duplicating features of Aadhaar, it is rightfully being used for weeding out bogus, duplicates, fakes, and for uniquely identifying individuals for delivery of benefits, services, and for tax administration. UID Scheme, in this sense, is a transformational homegrown IT project, and an important platform to improve the efficiency and transparency of various e-governance initiatives in the areas of food security, jobs, health, taxation, etc. The various arguments put forward by critic, objecting to the use of a single unique identifier across domains, for concerns of data security and compromising privacy of individuals, are untenable, as the Aadhaar Act, 2016 mandates most rigorous and strongest privacy protection provisions which are reflected in spirit and processes of UIDAI at all levels.

Hence, the UID Scheme with its net positive outcome, is recommended by the Committee to continue beyond 12th Five Year plan, i.e. March 2017. Committee further recommends that this scheme be regarded as work in perpetuity, in view of its increasing widespread use in multiple national activities.

Annexure 1

Aadhaar Act, 2016

330

To give statutory standing to UIDAI, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016") was passed by the Parliament on 16 March 2016 and published in the official gazette on 26 March 2016. UIDAI was notified as an Authority on 12th July, 2016, and the Chairperson and members of the Authority were appointed on 12 September 2016. On the same Day all sections of Aadhaar Act, barring Section 21, were notified. Subsequently, following regulations were notified on 14 September 2016:

1. Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations, 2016 (No. 1 of 2016)
2. Aadhaar (Enrolment and Update) Regulations, 2016 (No. 2 of 2016)
3. Aadhaar (Authentication) Regulations, 2016 (No. 3 of 2016)
4. Aadhaar (Data Security) Regulations, 2016 (No. 4 of 2016)
5. Aadhaar (Sharing of Information) Regulations, 2016 (No. 5 of 2016)

The powers and Functions of UIDAI as per Section 23 of Aadhaar Act, 2016

1. Define enrolment process for generation and assigning of Aadhaar numbers to individuals
2. Appointment of entities to operate the Central Identities Data Repository (CIDR)
3. Issue regulations pertaining to authentication of Aadhaar numbers
4. Issue regulations for maintaining and updating the information of individuals in the CIDR
5. Issue regulations on life cycle management of Aadhaar numbers
6. Specify the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services for which Aadhaar numbers may be used
7. Through regulations, specify terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation thereof
8. Establish, operate and maintain the CIDR
9. Through regulations, specify sharing the information of Aadhaar number holders, subject to the provisions of this Act
10. Call for information and records, conduct inspections, inquiries and audit of the operations for the purposes of this Act of the CIDR, Registrars, enrolling agencies and other agencies appointed under this Act
11. Through regulations, specify various processes relating to data management, security protocols and other technology safeguards under this Act
12. Through regulations, specify the conditions and procedures for issuance of new Aadhaar number to existing Aadhaar number holder
13. Through regulations, levy and collect fees or authorize the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act
14. Appoint such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act.
15. Promote research and development for advancement in biometrics and related areas, including usage of Aadhaar numbers through appropriate mechanisms.

-----*

Annexure 2

Synopsis of EFC approvals and Expenditures with Revised Cost Estimates*

Statement indicating approvals received and expenditure incurred upto 18th July 2017
(Amount in crores)

Sl No	Component	Approvals					Expenditure	RCT	Balance Available
		SFC	EFC B	EFC C	EFC IV	EFC V	Total		
1	Technology Infrastructure								
1 (a)	Capital Cost	8.57	379.06	2267.3			2654.93	1834.78	1070.12
1 (b)	Operational Cost	0	0	1486.2			1486.2	308.17	557.93
2	UBCC						0.00	0.00	
2 (a)	Capital Cost	0	4.00	1.87			5.87	0.00	5.87
2 (b)	Operational Cost	0	6.00	45.17			51.17	0.00	51.17
3	Support Infrastructure-operational costs								
3 (a)	Logistics	0	208.44	247.60	1549.00		1505.04	1146.33	858.59
3 (b)	Ashtar Sampark Kendra	0	131.36	117.62			249.98	31.76	67.50
3 (c)	Document Management System	0	0	381.80			381.80	321.80	161.01
3 (d)	Knowledge Management Portal	0	0	11.00			11.00	6.74	4.26
3 (e)	ICC	0	200.00	0			200.00	191.94	8.06
3 (f)	Testing, Training & Certification	0	0	49.32			49.32	1.12	48.20
3 (g)	Professional Services	13.38	95.94	204.16			313.48	126.58	187.20
3 (h)	Monitoring and Evaluation	0	0	132.00			132.00	10.19	121.81
4	Assistance to Registrars-operational cost (Enrolment, ICT, Incentive to RPL enrollees and Updation cost)	0	1450.00	178.12	2050.00	1265.00	4933.12	3831.70	1079.42
4 (a)	Enrolment cost		500.00	500	1600.00	1265.00	3865.00	3704.45	156.55
4 (b)	ICT Assistance and Capacity building in States		450.00	100			550.00	124.82	425.18
4 (c)	Incentive to RPL Enrollees		500.00	471.80			971.80	52.04	919.76
4 (d)	Updation cost				450.00		450.00	8.57	441.43

332

Statement indicating approvals received and expenditure incurred upto 18th July 2017 Annexure 1
(Amount in crores)

Sl No.	Component	Approvals					Total	Expenditure Total (2009 - 2017)	RCE	Balance Available
		SFC	EFC II	EFC III	EFC IV	EFC V				
5	Authentication Services- operational Cost	0	0	5.00			5.00	0.37		4.63
6	Aadhaar Enabled applications and Financial Inclusion	0	1.22	498.78			500.00	54.47		445.53
7	Construction of Buildings and Data Centers- Capital cost	5.20	83.00	87.06	247.16		372.42	401.03	83.26	54.38
8	Recurring Expenditure									
	Establishment cost of UID Hqs and ROs	120.16	493.79	401.55	50.00		1065.51	524.85		540.66
	Total	147.32	3013.01	5791.74	3436.16	1265.00	13663.22	8793.85	150.26	5019.67

*Revised Cost Estimate-

A) Rs 67 crore were approved in RCE by the Competent Authority in two tranches of Rs 15 crore and Rs 52 crore as on 17.09.2016 and 17.03.2016 respectively, as the approved EFC outlay fell short vis-à-vis contractual liabilities.

B) Rs 83.26 were approved in RCE by the Competent Authority in two tranches of Rs 63.25 crore and Rs 20.01 crore as on 16.04.2015 and 02.02.2017 respectively, as the approved EFC outlay fell short due to cost of land of HQ and DCs/Non DC buildings which was not taken into account at the time of Cabinet approvals, time over runs and due to addition of two additional floors in UIDAI HQ building under construction.

333

Annexure 3 (5)

UID as a Net Positive Scheme

As per DBT Mission, UIDAI has helped the government save Rs57,029 crore upto 2016-17 by way of Aadhaar linkage in various schemes. The schemes include DBT (PAHAL), PDS, NSAP and MGNREGA.

Benefit accrued on account for DBT/ Aadhaar since 2014 till 31st March 2017

			Upto 2015-16	Upto 2016-17
1	Petroleum & Natural Gas	PAHAL	21,584 crore	29,769 crore
2	Food & Public Distribution	PDS	10,191 crore	14,000 crore
3	Rural Development	MGNREGS	3,000 crore	11,741 crore
		NSAP	249 crore	399 crore
4	Others	Others	1,120 crore	1,120 crore
TOTAL			36,144 crore	57,029 crore

*(Source of Data: DBT Bharat Portal)

Considering the fact that use of Aadhaar is helping the government with direct financial savings, which are expected to accrue on a regular basis in future, it is a clear winner for the government. In addition, Integration of UIDAI in various governance initiatives has enabled the government to provide good and efficient governance to its people. Aadhaar has been linked with various applications, mentioned below, which have helped the government in bringing in more transparency in conduct of government business and enhancing ease of business that make a case for continuing UID Scheme beyond 12th Five Year Plan-

1. Aadhaar Enabled Biometric Attendance System (AEBAS) was launched in year 2015. As on 15 August 2017, the service is available at 662 organizations, to over 2.27 Lakh registered employees, operating at over 6000 active devices. It has been observed that due to AEBAS average presence in office has gone up thus filling gap in manpower requirements.
2. Jeevan Pramaan, which is a biometric authentication enabled 'Aadhaar-based Digital Life Certificate (DLC)' for pensioners, helps pensioners registered in the system to get 'life Certificate' needed for disbursement of pension, thus saving them from logistical hurdles in old age. As on 15th August 2017, with over 87 lakh registered users, about ~70 Lakhs pensioners have availed Authentication services of Aadhaar for Jeevan Pramaan in the current year so far.
3. Three-sign solution uses the existing e-KYC authentication mechanism under Aadhaar to verify the identity & address of the resident/signer and seek an online electronic signature from the issuing Certifying Authority (CA). Thus, a common man is enabled with digital signature facility and saves her from time taking and costly way of obtaining Digital Signature Certificate from licensed CCA.
4. DigiLocker is a cloud based platform for issuance and verification of documents & certificates digitally, thus eliminating the use of physical documents. It is a reality for Digital India's vision of providing citizens with a shareable private space on a public cloud and making all documents/certificates available on this cloud, thus helping in paperless governance. As on 15th August 2017, over 78 lakh users have registered with Digi Locker, storing over 98.65 lakh documents.

5. Mobile SIM issuance with e-KYC- Aadhaar has not only benefited the government, but Telecom Service Providers (TSP) have benefited by using e-KYC whereby the process of acquiring new SIM card has become paperless and reduced turnaround time for activation of SIM cards. Supreme Court of India has also acknowledged the benefits and ordered the TSPs to link all active mobile connections with Aadhaar in a year's time.
6. Pradhan Mantri Jan-Dhan Yojana (PMJDY) which was launched in August, 2014 has helped in financial inclusion. Aadhaar is used as the primary KYC document for opening a PMJDY Account and for delivering benefits to targeted beneficiaries. Use of Aadhaar e-KYC has brought a significant degree of comfort and convenience to the residents. As on 31st May 2017, over 28.44 crore accounts have been opened under the scheme of which over 18.97 crore are linked to Aadhaar Number.
7. Engagement of Bank Mitras (Banking Correspondents, BCs) serve as the main instrument of delivery of financial services using Aadhaar Authentication, thus helping in providing banking access to people in remote areas. There are more than 3.25 lakh BCs in July 2017.
8. Aadhaar in Securities Markets: Securities Market Regulator SEBI issued circular on 22-01-2016 on KYC, allowing Aadhaar Based e-KYC (OTP based up to Rs. 50,000 investments) as accepted mode of KYC. In case investments are above Rs. 50,000, resident needs to do biometric authentication based e-KYC. This has enabled small investors to open account and do small investments in a paperless manner.
9. Linking Universal Account Number (UAN) for EPFO with Aadhaar will help to clean EPFO database and help in hassle-free claim settlement and payment of benefits. As of 15th August 2017, of the 11.84 crore Accounts, over 1.94 crore have been linked to Aadhaar.
10. Acceptance of Aadhaar for issue of passport-Ministry of External Affairs, since May 2015, accepts Aadhaar as one of the PoI/PoA document by performing e-KYC of the applicant at the designated PSK. Till March 2017, over 1.36 crore e-KYC transactions have been performed by MEA for passport applications.
11. Use of Aadhaar authentication for e-verification of Income Tax Return-CBDT has launched e-verification service for Income Tax Returns. One of the options provided to resident is e-verification of Income Tax Return using Aadhaar OTP authentication. This was further strengthened on 31 March 2017 with making Aadhaar mandatory under section 139AA of Finance Act 2017 for FY 2017-18. As on 15th August 2017, over 3.27 crore PAN holders have linked and got their Aadhaar verified with CBDT. So far, about 1.20 crore Income Tax Payees have used Aadhaar based verification this year.
12. Aadhaar as an enabler in digital economy Aadhaar as an enabler in Digital cashless Economy - In addition to above benefits, Aadhaar is proving to be a foundation stone in digital cashless economy being promoted by the government post demonetization drive in November 2016. Aadhaar enabled Payment Systems, Bank Mitras and Aadhaar Pay applications as described below have yielded positive benefits to the society-
 - A. Aadhaar Enabled Payment System (AEPS)- has enabled residents to carry out banking transactions over handheld devices (micro-ATMs) carried by Business Correspondents (BCs) in remote corners of the country. Micro-ATMs provide doorstep services using Aadhaar and fingerprint of the resident. Aadhaar enabled basic banking transactions facilitated by BCs include:-
 - i. Balance Enquiry
 - ii. Cash Withdrawal
 - iii. Cash Deposit

iv. Aadhaar to Aadhaar Funds Transfer

At present 130 banks are live on AEPS ON-US and 88 banks are on OFF-US (inter-operable). As on 15th August 2017 over 75.57 crore successful transactions have taken place using AEPS across the banks. Last six month's average is 6.64 crore transactions per month that are happening across 3.25 lakh micro-ATMs in the field.

After the demonetization, use of AEPS has increased significantly. From 9th November 2016 till 15th August 2017 over 50.25 crore AEPS transactions were done in the field.

B. Aadhaar Pay is merchant version of AEPS. The Application works on a low cost android phone with single finger bio-metric device. It enables merchant to take cashless payment from his customers. Customer is only required to give his Aadhaar number, name of the bank (from where the money is to be deducted) and his fingerprint for authentication. The cost of this finger bio-metric device is about Rs. 2000. It enables merchant to take cashless payment from his customers. Launched on 14th April 2017, it is targeted to deploy about 20 lakh devices by September 2017. As of 15th August 2017, over 65 banks have become live on this system.

C. Pay to Aadhaar-It is a facility available on UPI platform integrated in BHIM app. It enables Person-to-Person (P2P) remittance using Aadhaar number of the recipient as financial address. The receiving Aadhaar number should be linked with his/her Aadhaar number. Launched early this year, it has been deployed by over 49 banks and enables over 51.67 crore Aadhaar linked bank a/c's to start receiving money using Aadhaar as financial Address.

336

Data Security and Privacy as provisioned in Aadhaar Act, 2016

1. Section 8 (4) provides that the Authority shall respond to an authentication query with a positive, negative or any other appropriate response, sharing such identity information excluding any core biometric information.
2. Section 8(2) (b) states that a requesting entity shall ensure that the identity information of an individual is used only for submission to the Central Identities Data Repository for authentication.
3. Chapter VI provides for a detailed framework for protection of information ensuring security, confidentiality and privacy of the data and the same standards are imposed on agencies, consultants, advisors or other persons appointed or engaged for performing any function of the Authority under this Act (Section 28).
4. Section 29 categorically states that no core biometric information, collected or created under this Act, shall be—
 - A. Shared with anyone for any reason whatsoever; or
 - B. Used for any purpose other than generation of Aadhaar numbers and authentication under this Act.
5. Section 30 applies the rigours of the I.T. Act, 2000 and the rules thereunder, whereby, Biometric Information is deemed to be Sensitive personal information.
6. Section 32 clarifies that the Authority shall not, either by itself or through any entity under its control, collect, keep or maintain any information about the purpose of authentication.
7. Section 33(2) provides disclosure in the interest of National Security, only upon a direction by an officer not less than the rank of a Joint Secretary, which is further 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.
8. Chapter VII lays down monetary penalties and imprisonment for unauthorized sharing of residents' identity information, failure to keep e-KYC data secure, failure to properly inform the residents about the use of their information, or failure to obtain their consent for authentication. The non-compliant individuals or entities may receive monetary penalty (up to one lakh rupees) and/or jail term (up to 3 years) which may vary depending upon the severity and impact of the violation. Some of the relevant sections on Penalties include:
 - A. Section 34: Penalty for impersonation at time of enrolment.
 - B. Section 35: Penalty for impersonation of Aadhaar number holder by changing demographic information or biometric information.
 - C. Section 36: Penalty for impersonation for collecting information.
 - D. Section 37: Penalty for disclosing identity information.
 - E. Section 38: Penalty for unauthorized access to the Central Identities Data Repository.
 - F. Section 39: Penalty for tampering with data in Central Identities Data Repository.
 - G. Section 40: Penalty for unauthorized use by requesting entity.
 - H. Section 41: Penalty for non-compliance with intimation requirements.
 - I. Section 42: General Penalty.
 - J. Section 43: Offences by Companies.
 - K. Section 44: Act to apply for offence or contravention committed outside India.

Annexure 5

Security of data in CIDR

337

The Central Identities Data Repository (CIDR) hosts the biometric data including encrypted enrolment packets, biometric template data and demographic data. UIDAI has followed a layered security approach to protect the sensitive information in CIDR. Following keys measures are taken in CIDR to protect the information.

1. **Robust Perimeter Security-** CIDR is divided into various zones based on risk and trust. These zones are protected by firewalls and perimeter zones are additionally protected by Intrusion Prevention systems (IPS) with clearly outlined rules based on business needs. The perimeter is continuously monitored by the Security Operations Centre (SOC) for security threats.
2. **Securing sensitive data in CIDR (Biometric and demographic)-** The biometric and demographic data is hosted in highly restricted zones within the CIDR (production zone). These zone are further restricted through firewalls within the CIDR and only necessary applications interact with these zones which are based on strict approvals.
3. **Storage of sensitive data in federated manner-** Biometric and Demographic data is stored in federated manner. Both biometric and demographic data cannot be found in a single database hence increasing the level of security of the information.
4. **Anonymization of data through reference ids-** The biometric data stored in various zones is only referenced through reference IDs and not through Aadhaar number. This increases the level of security multi-fold as to misuse the biometric data, one needs access to the respective Aadhaar number as well which is kept in a separate zone and strictly access controlled.
5. **Encryption-** All data is stored in the various databases in an encrypted format and the keys for encryption are managed using HSM devices.
6. **API based interaction-** Interaction with the various databases within CIDR is through APIs only hence restricting the level of access to various databases.
7. **Access control-** Access to the various infrastructures within CIDR by authorized personnel is highly restricted based on need and role. The access is periodically monitored by the administration.
8. **Identity and Access Management-** Identity and Access Management solution is implemented to control access to the servers and apply appropriate policies for access.
9. **Anti-virus and HIPS for the servers in CIDR-** Anti-virus and HIPS solution is deployed for all the servers in CIDR and the signatures are updated on daily/periodic basis as per the requirement.
10. **Continuous security monitoring through SIEM solution (Security Information and Event Management) in Security Operations Centre-** Security Analytics is implemented in CIDR to monitor real time security threats. All logs are monitored in SOC (Security Operations Centre) in the Headquarters for real time security threats.
11. **Periodic vulnerability assessments-** Quarterly vulnerability assessments are conducted to ensure Periodic vulnerability assessments are conducted.
12. **Technology developments-** Various security technology developments are continuously being monitored and UIDAI endeavours to deploy the best security technology solutions.

Organizational Security Measures taken by UIDAI

In addition to above, security measures at organizational level have been adopted as mentioned below which build a secure technology system-

1. ISO27001:2013 certification- UIDAI CIDR is ISO27001:2013 certified since 2015 and goes through yearly surveillance audits from STQC.
2. Information Security Policy- UIDAI has an Information security policy following the ISO27001:2013 standard.
3. Robust Security Organization- Assistant Director General (Information Security) has been designated as the Chief Information Security officer to drive information security measures in UIDAI.
4. Security monitoring agency- GRCP-SP (Governance, Risk, Compliance and Performance Service Provider) has been appointed to perform periodic monitoring of the security of internal and external ecosystem.
5. Third party security compliance-UIDAI ensures that conditions in various contracts signed with the ecosystem partners include compliance to information security policy of UIDAI. Periodic assessments are conducted for the ecosystem partners to ensure compliance on the Information Security policy.
6. As per UIDAI's CIDR facilities, Information Assets, Logistics and Infrastructure and Dependencies installed at UIDAI has been classified as Protected System under section 70 (1) of the Information Technology Act, 2000.

Data Security in collection and use of Aadhaar data

1. **Security of Enrolment system-** The Enrolment Client application is a desktop application provided by UIDAI which works in offline mode, and has all the features necessary to capture resident demographic details, do local validation, do local transliteration, capture biometric data, check biometric data quality and capture necessary audit details such as operator biometrics, location and time. Enrolment client software, also has built-in security features such as, in-memory data encryption, encrypted data storage, exports etc. The enrolment software is connected to CIDR via an authenticated and secured channel, each machine is registered in the system and uniquely defined, all operators and supervisors are Aadhaar trained and certified, they are registered with UIDAI and need to authenticate before processing enrolment. The biometric devices used for biometric data capture are connected via UIDAI provided "device manager" software embedded in the enrolment system. Every enrolment packet is biometrically signed by the operator ensuring traceability and non-repudiation. Further, every packet is reviewed and signed by a supervisor for data quality (review audits are captured electronically) which means every enrolment is traceable in terms of "who", "when", "where", "which agency", "which registrar", "who reviewed it", etc. Every packet is tamper proof and encrypted through PKI-2048 bit encryption at the time of capture. Encrypted Packets are securely uploaded to CIDR using customized software through registered upload stations initiated after a two factor authentication. These packets are "never" decrypted in transit.
2. **Security of Authentication System-** Aadhaar authentication system is also designed to ensure data security and privacy as ensued in the Aadhaar Act. The access to CIDR is available to authorized AUAs and KUAs through ASAs only which have established secured network connectivity with CIDR, for the purpose of authentication, in compliance with the Regulations, specifications, standards and technology architecture as prescribed by UIDAI. The information and data collected during authentication is immediately packaged and encrypted into Personal Identity (PID) block, as per the specifications laid down by the Authority, before any transmission. Each authentication transaction is traceable as a complete audit trail with device information and AUA/KUA/ASA time stamp is mandatorily maintained. UIDAI accepts only those authentication requests which are digitally signed by AUA/KUA/ASA. These agencies are also mandated to maintain information of all their authentication devices (send this information as part of authentication request to UIDAI), and transaction logs as prescribed by Aadhaar Authentication Regulations. UIDAI provides instant e-mail alert notifications to Aadhaar number holder for biometric authentication with details such as time of authentication, mode of authentication, the name of AUA through which authentication has happened and contact details of UIDAI. Therefore, in case of any issues with the transaction, Aadhaar number holder may approach UIDAI or the AUA. For better security, UIDAI also enables multi factor authentication to users.

Annexure 7

New Security Initiatives by UIDAI

1. **Secure ECMP Client:** UIDAI, in consultation with DRDO, is in the process of developing a secure USB based ECMP client for enrolment. A demonstration of the system was given to the Committee and the proposed solution is commendably secure and will further enhance the security of enrolment process. Committee suggests UIDAI to launch it at an earliest.
2. **Enrolment Centers with trusted partners:** It was informed that UIDAI has initiated a process of providing enrolment and update services by trusted partners only and hence it is in the process of locating Permanent Enrolment Centers at Post Offices, Nationalized Banks and Government offices to further enhance the security of enrolment process. Private operators involved in the enrolment process will be phased out in due course of time.
3. **Registered Devices:** UIDAI is in the process of introducing the concept of Registered Biometric Devices wherein each device will be uniquely identifiable, traceable, and biometrics captured by these devices will be encrypted at source. This will further enhance security at source of biometric data capturing. The key features of Registered Devices include
 - a. **Device Identification-** Every biometric device will have a unique identifier allowing traceability, analytics and fraud management
 - b. **Eliminating use of stored biometrics-** Biometric data is signed within the device using the provider key to ensure it is indeed captured live.
 - c. **A standardized and certified Registered Device Service** is to be provided by the device providers. This RD Service will encapsulate the biometric capture, signature & encryption of biometrics all within it. The RD Service forms the encrypted PID block before returning to the host application through local TCP/IP port.
4. **Virtual ID and Aadhaar token:** Aadhaar number sharing and seeding in many databases can potentially create data linking issues. Committee reviewed the work UIDAI has begun for tokenization and virtualization of the ID to address this issue. Committee is in full support of this effort.
5. **Secure QR Code:** UIDAI is in the process of providing secure QR code with signed information in Aadhaar letters and e-Aadhaar. This QR code would contain photograph and demographic information of the resident and the same can be verified using UIDAI provided scanner application for authenticity. The scanner application will be offered on Windows and Android platform to begin with. This feature will enable offline verification of Aadhaar details by user agencies and will help the user agencies in remote areas to verify Aadhaar information offline.
6. **Empanelment of Audit Agencies for Security Audit of AUAs/Sub-AUAs:** UIDAI has a long list of service providers and having an extensive ecosystem of audit agencies to ensure compliance of Aadhaar Act is very essential for UIDAI at this stage. UIDAI is in the process of empanelling various Audit Agencies to conduct security audit of AUAs/Sub-AUAs of Aadhaar ecosystem. This would ensure that various security policies and guidelines issued by UIDAI are strictly adhered to by these agencies.
7. **Formation of Security Review Committee:** UIDAI has formed a Security Review Committee, consisting of eminent members from Academia such as Indian Institute of Science, Indian Institute of Technology; Government agencies such as National Cyber Security Council, Defense Research and Development Organization etc., to provide expert guidance and support concerning Cyber Security matters for UIDAI internal and external ecosystem on an ongoing basis.

341

8. Empanelment of Certification Agencies to certify Auth applications of AUAs/Sub-AUAs: UIDAI is in the process of empanelling various certification agencies to certify various applications developed by AUAs/Sub-AUAs of Aadhaar ecosystem. This would ensure that various security policies and guidelines issued by UIDAI are strictly adhered to. Once certified, the list of certified applications will be available on UIDAI website for the information of the residents.

Annexure 8

342

Justification for Continuation of scheme

The work of UIDAI on giving Aadhaar numbers to the residents of India, and offering Aadhaar updation services and digital authentication services, is a work in perpetuity. UIDAI needs to continue its operations for the following reasons:

1. To continue allocating Aadhaar number to new-borns (nearly 2 Cr children are born every year) and to provide for mandatory biometric updates to similar number of children who become eligible for biometric updates at the age of 5 and 15 years of age.
2. To continue providing for Update services to residents who need to update their Aadhaar details due to life event changes like marriage, movement to new locations, etc. This is also essential for UIDAI to ensure that Aadhaar data of the residents stored in the CIDR is accurate and up-to-date for enabling Aadhaar authentication for various Government and Non-Government Services like Subsidy Benefits, Pensions, Scholarships, Social Benefits, Banking, Insurance, Taxation, Education, Employment, Healthcare, etc.
3. To continue providing authentication services to various Central and State government Ministries which are using or may decide to use Aadhaar, as per Section 7 of Chapter III of the Aadhaar Act, 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, or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment.
4. To continue facilitating Aadhaar related services for financial inclusion and banking where, Aadhaar serves as a financial address of the resident and funds can be transferred to Aadhaar linked account of a resident through Aadhaar Payment Bridge (APB) and Aadhaar Enabled Payment System (AEPS) operated by National Payments Corporation of India.
5. To continue providing digital authentication and eKYC services to various government and private agencies through its Authentication ecosystem comprising of AUA/KUA and ASA.

-----****-----

30-343

Annexure R-12

Ajay Bhushan Pandey

Chief Executive Officer at Unique Identification Authority of India (UIDAI)

Summary

N/A

Experience

Chief Executive Officer at Unique Identification Authority of India (UIDAI)

July 2016 - Present

Heading Aadhaar program in India

Director General at Unique Identification Authority of India (UIDAI)

September 2015 - July 2016 (11 months)

Heading Aadhaar program in India

Deputy Director General at Unique Identification Authority of India (UIDAI)

September 2010 - August 2015 (5 years)

Secretary, Information Technology Department

February 2009 - April 2011 (2 years 3 months)

Managing Director

October 2006 - January 2009 (2 years 4 months)

Secretary Information Technology

October 2004 - June 2006 (1 year 9 months)

Secretary to Chief Minister Maharashtra

August 2003 - December 2004 (1 year 5 months)

Education

University of Minnesota-Twin Cities

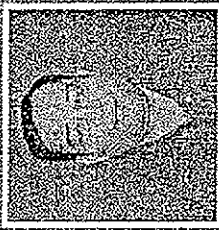
PhD, Computer Science, 2000 - 2004

University of Minnesota-Twin Cities

M S, Computer Science, 1998 - 2000

Indian Institute of Technology, Kanpur

B Tech, Electrical Engineering, 1978 - 1983



Dr. Gulshan Rai

Director General, CERT-In (Indian Computer Emergency Response Team)

Biography

Dr. Gulshan Rai has over 25 years of experience in different areas of Information Technology which include Cyber Security, e-Governance, Legal Framework and the Information Technology Act for e-commerce, and several related fields. At present, he is Director General, CERT-In (Indian Computer Emergency Response Team) and Group Coordinator of E-Security and Cyber Law Division in the Ministry of Communications and Information Technology. Prior to this, he was Executive Director, ERNET India for over 7 years and he was instrumental in setting up of the first large scale education and research network in close collaboration with the leading educational and research institutions in the country.

Dr. Rai has been working since 1998 in the area of evolving legal framework to address issues arising out of cyberspace. His sustained efforts in the area has resulted in second Technology Legislation in the History of India i.e. Information Technology Act and recent amendments in the Act.

Dr. Rai is particularly focused on developing security capabilities in the country through increased security education programs.

Cyber Security has emerged a very important area. The country is in the process of implementing few crucial projects, for example, setting up of National Cyber Coordination Centre, Security Testing Infrastructure Security Framework for E-Governance, Infrastructure and Human Resource Development in the country. National Security Council has already approved these projects besides the National Cyber Security Policy is also under approval. The policy needs to be implemented in the country. All these projects require experience at the national and international level and knowledge in the area and continuity so as to implement in a time targeting manner. The entire investment is expected to be Rs. 2000 crores in the next three years.

Rajat Moona

Professor at IIT Kanpur

Summary

I have had a variety of professional experience - ranging from teaching and research to development of technologies and standards. I love to build systems and my goal is to see more and more deployment of technologies to make life easier.

Specialties: Education, Research, Training, Technology development and deployments, Cyber Security, Smart Cards and e-tokens, RFID.

Experience

Director

March 2017 - Present

Professor at IIT Kanpur

April 1991 - Present

I started my professional career from IIT Kanpur right after my PhD. I have been teaching, doing research and have had a rich interactions with various industries and Government. Have been on several national committees to guide policy makers on technical fronts.

Director General at CDAC

June 2011 - March 2017 (5 years 10 months)

CDAC is the Govt of India R&D organization under the ministry of Communication and Information Technology for research in advanced electronics and computing technology. It is spread over 11 cities in India with headquarters at Pune. In this assignment, I need to define the research directions for CDAC and work with various research groups. CDAC has about 3000 employees of high calibre and excellent grasp over contemporary research.

Sr. Engineering Manager at Mentor Graphics

May 2002 - July 2004 (2 years 3 months)

Worked at Hyderabad Research Facility of Mentor Graphics. Supervised the development of Seamless-ASAP product.

Sr. Engineering Manager

2002 - 2004 (3 years)

Mentor Graphics India is a subsidiary of Mentor Graphics Corp. The company has business in the area of the EDA design tools. I worked in the Seamless ASAP group there.

346

Visiting Researcher at MIT

May 1994 - February 1995 (10 months)

Visited the Lab for Computer Science (CSG Group) and worked with Prof. Arvind's Research Group under a DST fellowship.

Scientific Officer

October 1989 - March 1990 (6 months)

Right after my PhD from the IISc Bangalore, I worked there on continuing to build more infrastructure to the parallel machine designed as part of the PhD problem. I worked on porting the AT&T SVT3.2 unix OS on this machine with constructions to do parallel computation.

Education

Indian Institute of Science (IISc)

PhD, Computer Science, 1985 - 1989

IIT Kanpur

BTech, EE, July 1981 - May 1985

Sri Vishnu Inter College

High School, 1976 - 1981

347

Dr. H Krishnamurthy

Dr. HR Krishnamurthy is a professor with the Department of Physics at the renowned Indian Institute of Science Bangalore. He completed his MSc at IIT Kanpur and his MS and PhD(1978) from Cornell University, USA. His research interests include Theoretical condensed Matter Physics, with a focus on strongly interacting quantum and classical many-body systems, especially quantum impurity physics and theories of strong correlation phenomena in solids.

Some of his notable positions include

- Visiting Associate, Department of Physics and the Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA, USA
- Visiting Professor, Physics Department, Harvard University, Cambridge, Mass, USA
- Visiting Professor, University of California, SantaCruz, Riverside and Davis, CA USA
- Elected Fellow of the American Physical Society (APS), 2015, Member, Management Board, International Centre for Theoretical Sciences, India, 2008
- Holds 65 publications to his name and 25+ students who have completed(or undergoing) PhD under his Guidance

348

Dr. Manindra Agarwal

Dr. Manindra Agrawal is a professor at the Department of Computer Science and Engineering and the Deputy Director at the Indian Institute of Technology, Kanpur. He was the recipient of the first Infosys Prize for Mathematics and the Shanti Swarup Bhatnagar Award in Mathematical Sciences in 2003. He has been honored with Padma Shri in 2013. Manindra Agrawal obtained a B.Tech. from IIT Kanpur (1986 batch) and a Ph.D. from the same institute.

Some of his other notable achievements include:

- Awards - Clay Research Award (2002), S S Bhatnagar Prize (2003) ICTP Prize (2003) Fulkerson Prize (2006) Gödel Prize (2006) G.D. Birla Award for Scientific Research (2009) Padma Shri (2013))
- Co-created the AKS primality test with Neeraj Kayal and Nitin Saxena, for which he and his co-authors won the 2006 Fulkerson Prize
- Designed private-key encryption algorithms for Indian Navy and Air Force. These algorithms are being used by the armed forces to secure their communications.
- Humboldt Fellow at the University of Ulm, Germany
- Appointed as the N. Rama Rao Chair Professor and a visiting scholar at the Institute for Advanced Study.

349

Sandeep Shukla

Head of the Department, Computer Science and Engineering at Indian Institute of Technology, Kanpur

Summary

My PhD is on theoretical analysis, complexity analysis and mapping of algorithmic aspects of formal verification. After my PhD, I worked in a telecommunications network management software lab where I developed distributed algorithms and their implementations for network management systems, and did research on middleware based distributed object technology. However, after 2 years in the telecom industry, I went back to my roots, and joined the formal verification team at Intel, working on the formal property verification of the ITANIUM processor microarchitecture, and while being at Intel, I took up interest in high level system modeling languages, simulation, and high level/behavioral synthesis. I was in a pilot team of experts for looking into various possible system design languages for a future generation IA64 processor design team. Eventually, I became a part of an IA64 Platform architecture group where I had to formally specify IA64 bus protocols and automatically generate checkers etc.

In 2001, after 4 years of industry exposure, I decided to go back to academia. So I joined a post doctoral research associate position at the center for embedded computer systems at the University of California at Irvine. There, I started working on dynamic system level power management, IP composition for SoC design, formal methods for system design and other problems related to embedded system design. In fall 2002, I joined Virginia Polytechnic and State University as an assistant professor of computer engineering. My research lab is called FERMAT (Formal Engineering Research with Models, Abstractions and Transformations) whose website <http://fermat.ece.vt.edu> will provide more details of our research.

Specialties: Teaching, Research, research supervision, project management, mentoring of students

Experience

Head of the Department, Computer Science and Engineering at Indian Institute of Technology, Kanpur
February 2017 - Present

Coordinator, Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructure
April 2016 - Present

<https://security.cse.iitk.ac.in>

Poonam and Prabhu Goel Chair Professor and Dr. Deep Singh and Daljeet Kaur Faculty Fellow at Indian Institute of Technology Kanpur
2015 - Present

<http://www.cse.iitk.ac.in/users/sandeeps/>

Editor in Chief

350

November 2013 - Present

Professor at Virginia Tech

April 2012 - July 2015 (3 years 4 months)

At the Virginia Tech National Capital Region Campus at Falls Church, VA

Director, Center for Embedded Systems for Critical Applications

August 2010 - July 2012 (2 years)

I took up the responsibility to direct the center. I was the deputy director before.

Associate Professor

August 2007 - April 2012 (4 years 9 months)

Teaching, Research, Advising Graduate students, post doctoral fellows and undergraduate research students, mentoring other faculty, direct a center

Humboldt Bessel Award visiting faculty

April 2009 - August 2009 (5 months)

Worked on Combining Polychronous and Synchronous language theories

Visiting Professor at INRIA

July 2008 - April 2009 (10 months)

Worked on Polychronous Language application to System Level Design

AFRL Information Institute Visiting Faculty

May 2008 - July 2008 (3 months)

Developed and architected a Software Synthesis Tool

ASEE/Air Force Summer Faculty Fellow

May 2007 - August 2007 (4 months)

Worked on embedded-software for a special processor

Assistant Professor at Virginia Tech

August 2002 - July 2007 (5 years)

Teach, research

Graduate Research Assistant at State University of New York at Albany

June 2004 - December 2006 (2 years 7 months)

Research on Formal Methods

Visiting Researcher at MIT

June 2006 - August 2006 (3 months)

Worked on Understanding Dataflow Computing Architecture and their applications to GALS design

ASEE Senior Summer Faculty Fellow

351

2005 - 2005 (1 year)

Research on relating SCR specification language to synchronous languages

Research Associate

April 2001 - August 2002 (1 year 5 months)

Research Faculty at the Center for Embedded Computer Systems

Staff Design Engineer at Intel Corporation

March 1999 - March 2001 (2 years 1 month)

Formal Verification of Bus Cluster of Itanium chip, System Level Design Languages, Bus Protocol
Formalization, and Synthesis of Checkers

Principal Member of Technical Staff

March 1997 - March 1999 (2 years 1 month)

Telecommunication Network Management Software Development, Middleware based Rearchitecture of
Existing Client/Server Systems

Summer Member of Technical Staff at Bell Laboratories

May 1996 - August 1996 (4 months)

Worked on a formal verification tool development

Graduate Teaching Assistant at State University of New York at Albany

September 1992 - June 1994 (1 year 10 months)

Teach Tutorial Classes on Discrete Mathematics, Programming Language Theory etc.

Student at Jadavpur University

1987 - 1992 (6 years)

Study Bachelors of Computer Science and Engineering

Education

University at Albany, SUNY

PhD, Computer Science, 1992 - 1997

State University of New York - System

MS, Computer Science, 1992 - 1995

Jadavpur University

BE, Computer Science and Engineering, 1987 - 1991

Activities and Societies: Contributed Poetry to Faculty of Engineering Magazine, acted as JR (Journal representative) for my class.

St. Xavier's College

Higher Secondary certificate, Physical Sciences, 1985 - 1987

Activities and Societies: Bengali Literature Society

New Alipore Multipurpose School

School leaving certificate, General Studies, 1974 - 1985

352 ✓

Activities and Societies: Quiz

Honors and Awards

Google Scholar Profile, Research Gate Profile, ACM Distinguished Scientist, IEEE Fellow, Ramanujan Fellow, ACM Distinguished Speaker

953

Subhashis Banerjee: BIO-DATA

1

BIO-DATA

1 Name:

Subhashis Banerjee

2 Present Address:

Professor
Department of Computer Science and Engineering
Indian Institute of Technology
New Delhi 110016

3 Academic Qualifications:

Ph.D Thesis: On Stochastic Relaxation Paradigms for Computational Vision
Electrical Engineering
Indian Institute of Science, Bangalore
1989

ME Electrical Engineering
Indian Institute of Science, Bangalore
1984

BE Electrical Engineering
Jadavpur University, Calcutta
1982

4 Details of Employment

Professor
Department of Computer Science and Engineering
Indian Institute of Technology, Delhi
From January 2000 till date

Ministry of Urban Development Chair Professor, since November 2015.

Microsoft Chair Professor, from May 2010 to March 2013.

Naren Gupta Chair Professor, 2004-2006.

Head, Computer Services Center, from September, 2009 to August, 2012

Head, Department of Computer Science and Engineering, from September, 2004 to August, 2007.

Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology, Delhi
From August 1997 to January 2000

354

Subhashis Banerjee: BIO-DATA

2

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology, Delhi
From April 1990 to August, 1997

Lecturer
Department of Computer Science and Engineering
Indian Institute of Technology, Delhi
From December 1989 to March 1990

5 Field of Specialization

Computer Vision, Pattern Recognition, Image Based Rendering and Real-time Embedded Systems.

6 Awards/Recognition

1. IIT Delhi Teaching excellence award, 2011.
2. Ministry of Urban Development Chair Professorship, Department of Computer Science and Engineering, IIT Delhi, since 2016.
3. Microsoft Chair Professorship, Department of Computer Science and Engineering, IIT Delhi, 2010-2013.
4. Naren Gupta Chair Professorship, Department of Computer Science and Engineering, IIT Delhi, 2004-2006.
5. Best paper of the year (July 94 - June 95) "

Issue on Robotics and Automation, 25(1),

pp. 174-208, March 1995.

6. Young Scientist award of the Department of Atomic Energy, 1994.

7 Ph.D. guided/on-going

- Britty Baby, (ongoing)
Ego-motion based depth estimation using endoscopic cameras in neurosurgical simulation and training,
jointly with Ashish Suri (AIIMS) and Prem Kalra of Dept. CSE, IITD.
- Suvam Patra, (ongoing)
3D registration and reconstruction from multi-modal data,
jointly with Prem Kalra of Dept. CSE, IITD.
- Brojeshwar Bhowmick, (ongoing)
Dense and large scale 3D reconstruction,
jointly with Prem Kalra of Dept. CSE, IITD.

Subhashis Banerjee: BIO-DATA

- Chetan Arora, 2013
On Graph-cut algorithms in Computer Vision,
jointly with Prem Kalra and S. N. Maheshwari of Dept. CSE, IITD.
- Tanveer Faruque, 2012
Novel Space-time Activity Modelling Techniques for Video Surveillance,
jointly with Prem Kalra of Dept. CSE, IITD.
- Ayesha Choudhary, 2011
Detection of unusual activities in Videos,
jointly with Santanu Chaudhury of Dept. EE, IITD.
- Uma Mudenagudi, 2007
Markov Random Field Models for Super Resolution in Space and Time,
jointly with Prem Kalra of Dept. CSE, IITD.
- Subhajit Sanyal, 2006
Interactive Image-Based Modeling and Walkthrough Planning,
jointly with Prem Kalra of Dept. CSE, IITD.
- Parag Chaudhuri, 2005
A Framework for View-Dependent Character Animation,
jointly with Prem Kalra of Dept. CSE, IITD.
- Shoma Chatterjee, 2002
"Vision Based Motion Image Compression"
jointly with K. K. Biswas of Dept. CSE, IITD.
- Sumantra Dutta Roy, 2000
"Active Object Recognition through Next View Planning"
jointly with Santanu Chaudhury of Dept. EE, IITD.
- Navin Rajpal, 1998 "Development of Object Recognition Systems using Invariant Feature
based Indexing"
jointly with Santanu Chaudhury of Dept. EE, IITD.
- also guided the Ph. D research of G. Sudhir who completed his Ph.D from CARE, IITD
in 1994, and formally was a student of Prof. K. K. Biswas, DCSE and Dr. R. Bahl,
CARE. "Relaxation Algorithms for Computer Vision".

8 Courses taught

- Introduction to Computers and Programming
- Introduction to Computer Science
- Data Structures
- Discrete Structures
- Numerical Algorithms

356

Subhashis Banerjee: BIO-DATA

4

- Design Practices in Computer Science
- Operating Systems
- Computer Graphics
- Pattern Recognition and Image Processing
- Digital Image Analysis
- Mathematical Foundations of Computer Science
- Logic and Functional Programming
- Computer Vision
- Neural Networks and Machine Learning
- Quantum Computation and Information Theory
- Machine Learning and Data Mining
- Simultaneous localization and mapping (special module)
- Deep Learning (special module)

9 Research

9.1 Ph.D Research

'On Stochastic Relaxation Paradigms for Computational Vision', 1984 - 1989.

Department of Electrical Engineering, Indian Institute of Science, Bangalore.

Supervisors: Prof. Y. V. Venkatesh, Prof. K. R. Ramakrishnan and Prof. P. S. Sastry.

9.2 Research at IITD

Please see

1. <http://www.cse.iitd.ac.in/~suban>
2. <http://www.cse.iitd.ac.in/~suban/lab>
3. <http://www.cse.iitd.ac.in/~suban/students.html>

9.3 Sponsored research (2010-2015)

1. AIIMS-IITD Centre of Excellence for Neuro-engineering.

Coordinators: Ashish Suri (AIIMS) and Subhashis Banerjee.

Funding agency: DBT

Budget: Rs. 10,00,00,000

Duration: 2017-

2. Four problems related to ADAS

357

Subhashis Banerjee: BIO-DATA

5

PI: Subhashis Banerjee.

Others: Chetan Arora (IIITD) and Uma Mudanagudi (BVBCET)

Funding agency: Continental Automotive

Budget: Rs. 30,00,000

Duration: 2016-2017.

3. Two ongoing collaborative projects (as Co-PI) with Department of Neurosurgery, AIIMS with major part of the funding at AIIMS:
 - (a) Evaluation of development of neurosurgery skills by hands-on skills training and interactive virtual training (Rs. 1.49,00,000).
 - (b) IIT Delhi as Repository Centre for Archival transmission and Computing (Rs. 1.50,00,000).

4. Creation of central computing infrastructure for universities.

Chief Investigator: Huzur Saran

Co-investigator: Sorav Bansal, Subhashis Banerjee, R. S. Mani (NIC).

Funding agency: MHRD (NMEICT).

Budget: Rs. 40,00,00,000

Duration: 2012 -

5. Research group on computer graphics and vision, Indo-German Max Planck Centre for Computer Science.

Investigators: Prem Kalra, Subodh Kumar, Subhashis Banerjee, Hans-Peter Seidel, Michael Wand and Christian Theobalt.

Funding agency: DST, Bundesministerium für Bildung und Forschung (BMBF, Federal Ministry of Education and Research) and the Max-Planck-Gesellschaft (MPG, Max Planck Society).

Duration: 2010 -

6. Similarity measures and their optimization for video analysis and editing.

Chief Investigator: Subhashis Banerjee.

Co-investigator: P. J. Narayanan (IIIT Hyderabad), Shmuel Peleg (Hebrew University, Jerusalem) and Michael Werman (Hebrew University, Jerusalem).

Funding agency: DST (Indo-Israel Project).

Budget: Rs. 5,00,000

Duration: 2012 - 2014

7. Acquisition, Representation, Processing and Display of Digital Heritage Sites.

Chief Investigator: Prem Kalra

Co-investigator: Subodh Kumar, Subhashis Banerjee, others.

Funding agency: DST

Budget: Rs. 57,00,000

358

Subhashis Banerjee: BIO-DATA

6

Duration: 2010 - 2013

8. Immersive Environment for Tele-operation (Sub project No. 1 under the main project RP02346).

Chief Investigator: Prem Kalra

Co-investigator: Subodh Kumar, Sumantra Dutta Roy, Santanu Chaudhury, Subhashis Banerjee, others.

Funding agency: BRNS, DAE

Budget: Rs. 1,53,34,000

Duration: 2010 - 2015

9. Vision-Guided Control of a Robot Manipulator (Sub project No. 3 under the main project RP02346).

Chief Investigator: Sumantra Dutta Roy

Co-investigator: Santanu Chaudhury, Prem Kalra, Sudipto Mukherjee, Subhashis Banerjee, others.

Funding agency: BRNS, DAE

Budget: Rs. 1,44,34,000

Duration: 2010 - 2015

10. Large scale data processing and visualization

Chief Investigator: Subodh Kumar

Co-investigators: Subhashis Banerjee, Prem Kalra, Niloy J Mitra, Kolin Paul, Sandeep Sen, Santanu Chaudhury (EE), Rajinder Bahl (CARE), Sanjeev Sanghi (AM), Om P Sharma (CAS)

Funding agency: Naval Research Board

Budget: Rs. 39,74,100

Duration: 2008-2010

11. Visual enhancement, manipulation and retargeting of videos

Chief Investigator: Subhashis Banerjee

Co-investigators: P J Narayanan (IIT Hyderabad), Uma Mudanagudi (BVB College, Hubli) and Prem Kalra

Funding agency: Naval Research Board

Budget: Rs. 25,40,000 (Rs. 8,00,000 for IITD)

Duration: 2008-2010

359

Subhashis Banerjee: BIO-DATA

7

10 Other Academic and Professional Activities

1. On the editorial board of the *International Journal of Computer Vision*, Springer, 2004-2014.
2. On the editorial board of the *Computers and Graphics*, Elsevier, from 2007 - 2010.
3. Mentor and on Board of Directors of Kritikal Solutions Private Limited, a TBIU start-up company of IIT Delhi.
4. Helped Kritikal Solutions Pvt. Ltd. develop two successful products - *Vehicle underside scanner* (deployed at the Rashtrapati bhavan, Hyderabad airport and over 30 other installations) and *Automatic license plate reader* (to be deployed at several toll plazas across the country and possibly by the Delhi traffic department).
5. Regular review work for International Conference on Computer Vision (ICCV), Computer Vision and Pattern Recognition (CVPR), European Conference on Computer Vision (ECCV), International Journal of Computer Vision (IJCV), Journal of Image and Vision Computing, IEEE Transactions PAMI and SMC, and others.
6. Served on faculty selection committees of IITs at Delhi, Bombay, Kharagpur, Kanpur, Madras, Guwahati, Mandi, Ropar, Patna, Gandhinagar, Indore and Rajasthan; IISc Bangalore; IIIT Delhi, BHU; ISI Kolk, Ili University, Viswa Bharati and several others.
7. Invited speaker at the Workshops on *Graphs and Geometry* organised by TIFR and BHM at IIT BHU, IIT Guwahati, NIT Rourkela, Thapar Institute Patiala and BESU Shibpur, WB, Kashmir University and Sikkim University in the period 2010 - 2015.
8. Invited talk on *Graph cut algorithms in Computer Vision* at the Digital Video Processing Workshop at IIT Madras, December 2012.
9. Invited talk on *Projective Geometry in Computer Vision* at the Centenary Workshop of Department Electrical Engineering, IISc Bangalore, 2011.
10. Invited talks at IIT Bombay, IIT Kharagpur, IIT Kanpur, IISc Bangalore, Jadavpur University, ISI Kol, I-Informatik, Saar Bruecken and Microsoft Research (Redmond) between 2010-2016.

11 Publications (since 2000):

Books

- *View-dependent Character Animation*. Parag Chaudhuri, Prem Kalra and Subhashis Banerjee. Springer Research Monograph (ISBN: 1846285917), 2006.

Manuscripts

1. Suvam Patra, Kartikeya Gupta, Faran Ahmad, Chetan Arora, Subhashis Banerjee. *Batch based Monocular SLAM for Egocentric Videos*, March 2017. (arXiv, July 2017).

Journals

360

Subhashis Banerjee: BIO-DATA

8

1. Brojeshwar Bhowmick, Suvain Patra, Avishek Chatterjee, Venu Madhav Govindu, Subhashis Banerjee. *Divide and Conquer: A Hierarchical Approach to Large-scale Structure-from-Motion*. Computer Vision and Image Understanding (CVIU), Volume 157, pp. 190-205, April 2017.
2. Chetan Arora, Subhashis Banerjee, Prem Kalra and S. N. Malleshwari. *Generalized Flows for Optimal Inference in Higher Order MRF-MAP*. IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume: 37, Issue: 7, pp. 1323 - 1335, July 2015.
3. M Tripathi, R. C. Deo, A. Suri, V. Srivastav, B Baby, S. Kumar, P. Kalra, S. Banerjee, T. S. Roy, S. Lalwani. *Quantitative Analysis of Kawase's Triangle versus Modified Dolenc Kawase Rhomboid Approach for Middle Cranial Fossa Lesions with Variable Antero-posterior Extension*. Journal of Neurosurgery, 2015.
4. M Tripathi, R. C. Deo, A. Suri, V. Srivastav, B Baby, S. Kumar, P. Kalra, S. Banerjee, T. S. Roy, S. Lalwani. *Quantitative Analysis of Variable Extent of Anterior Clinoidectomy with Intradural and Extradural Approaches: 3-Dimensional Analysis and Cadaver Dissection*. Neurosurgery, March 2015. Suppl 2:147-61.
5. P. Jotwani, V. Srivastav, M. I. C. Deo, B. Baby, N. Damodaran, R. Singh, A. Suri, M. Bettag, T. S. Roy, C. Busert, M. Mehlitz, S. Lalwani, K. Garg, K. Paul, S. Prasad, S. Banerjee, P. Kalra, S. Kumar, B. S. Sharma, A. K. Mahapatra. *Free-access Open-source e-Learning in Comprehensive Neurosurgery Skills Training*, Neurol India 2014 July-August 62 (4): 352-61.
6. A. Suri, M. Bettag, M. I. C. Deo, T. S. Roy, S. Lalwani, C. Busert, M. Mehlitz, B. Baby, V. Srivastav, R. Singh, S. Kumar, P. Kalra, S. Banerjee, K. Paul, S. Prasad. *Simulation in Neurosurgery in India-NETS*. CNS Quarterly 2014;3:23-26.
7. Tanveer A. Faruque, Subhashis Banerjee, Prem K. Kalra. *Unsupervised discovery of activity correlations using latent topic models*, The Visual Computer 27(12): 1071-1082 (2011). (selected from among the best papers of ICVGIP 2010).
8. Uma Mudenagudi, Subhashis Banerjee and Prem Kalra. *Space-time Super-Resolution Using Graph-cut Optimization*. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33 No. 5, pp. 995-1008, May 2011
Pre-print: <http://www.computer.org/portal/web/csdl/doi/10.1109/TPAMI.2010.167>. August, 2010.
9. Parag Chaudhuri, Prem Kalra and Subhashis Banerjee. *Reusing View-Dependent Animation*. The Visual Computer. Vol. 23. No. (9-11), pp. 707-719. September, 2007.
10. Subhajit Sanyal, Prem Kalra and Subhashis Banerjee. *Designing Quality Walkthroughs*. Computer Animation and Virtual Worlds. Vol. 18, No. 4-5, pp. 527-538, September, 2007.
11. Sumantra Dutta Roy, Santanu Chaudhury and Subhashis Banerjee. *Recognizing Large Isolated 3-D Objects through Next View Planning using Inner Camera Invariants*. IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics. Vol. 35. No. 2, pp. 282 - 292, April, 2005.

361

Subhashis Banerjee: BIO-DATA

9

12. Puneet Sharma, Angshuman Parashar, Subhashis Banerjee and Prem Kalra. *An Uncalibrated Lightfield Acquisition System*. Journal of Image and Vision Computing, Vol. 22, No. 14, pp. 1197-1202, December, 2004.
13. Parag Chaudhuri, Prem Kalra and Subhashis Banerjee. *A System for View-Dependent Animation*. Computer Graphics Forum. Vol. 23, No. 3, pp. 411 - 420, September, 2004.
14. Sumantra Dutta Roy, Santanu Chaudhury and Subhashis Banerjee. *Active Object Recognition through Next View Planning: A Survey*. Pattern Recognition, Vol. 37, No. 3, pp. 429-446, March, 2004.
15. Aditya Ramamoorthy, Namrata Vaswani, Santanu Chaudhury and Subhashis Banerjee. *Recognition of dynamic hand gestures*. Pattern Recognition, Vol. 36, No. 9, pp. 2069-2081, September, 2003.
16. Sumantra Dutta Roy, Santanu Chaudhury and Subhashis Banerjee. *Aspect Graph Construction with Noisy Feature Detectors*. IEEE Transactions Systems, Man and Cybernetics - Part B: Cybernetics, Vol. 33, No. 2, pp. 340-351, April, 2003.
17. Namita Gupta, Pooja Mittal, Sumantra Dutta Roy, Santanu Chaudhury and Subhashis Banerjee. *Developing a Gesture-based Interface*. IETE Journal of Research: Special Issue on Visual Media Processing, Vol. 48, No. 3 and 4, pp. 237-244, August, 2002.
18. Rohit Jaivant Kate, Prem Kalra and Subhashis Banerjee. *Towards an Automatic Approach for View Dependent Geometry*. International Journal of Image and Graphics, Vol. 2, No. 3, pp. 413-423, July, 2002.
19. Sumantra Dutta Roy, Santanu Chaudhury and Subhashis Banerjee. *Aspect Graph based Modeling and Recognition with an Active Sensor: A Robust Approach*. Proc. Indian National Science Academy. Part A. Special Issue on Image Processing, Vision and Pattern Recognition, Vol. 67, No. 2, pp. 187-206, March, 2001.
20. Sumantra Dutta Roy, Santanu Chaudhury and Subhashis Banerjee. *Isolated 3D Object Recognition using Next View Planning*. IEEE Transactions Systems, Man and Cybernetics - part A. Vol. 30, No. 1, pp. 67-76, January, 2000.

Conferences

20. Shashank Yadav, Suvam Patra, Chetan Arora, Subhashis Banerjee, *Deep CNN with Color Lines model for unmarked road segmentation*, IEEE International Conference on Image Processing (ICIP 2017), Beijing, September 2017.
21. Suvam Patra, Himanshu Aggarwal, Himani Arora, Chetan Arora, Subhashis Banerjee. *Computing Egomotion with Local Loop Closures for Egocentric Videos*. IEEE Winter Conference on Applications of Computer Vision (WACV), March 2017.
22. Brojeshwar Bhowmick, Suvam Patra, Avishek Chatterjee, Venu Madhav Govindu, Subhashis Banerjee. *Divide and Conquer: Efficient large-scale structure from motion using graph partitioning*. ACCV, November 2014, Singapore.
23. Chetan Arora, Subhashis Banerjee, Prem Kumar Kalra, S. N. Maheshwari. *Fast Approximate Inference in Higher Order MRF-MAP Labeling Problems*. CVPR 2014: 1338-1345.

362

Subhashis Banerjee: BIO-DATA

10

24. Tanveer A. Faruque, Subhashis Banerjee, Prem Kumar Kalra. *Unsupervised Discovery of Activities and Their Temporal Behaviour*. AVSS 2012: 100-105.
25. Ayesha Choudhary, Tanveer A. Faruque, Subhashis Banerjee, Santanu Chaudhury. *Discovering Activities and Their Temporal Significance*. AVSS 2012: 240-245.
26. Chetan Arora, Subhashis Banerjee, Prem Kalra, S. N. Maheshwari. *Generic Cuts: An Efficient Algorithm for Optimal Inference in Higher Order MRF-MAP*. ECCV (5) 2012: 17-30.
27. Dakshita Khurana, Surabhi Sankhla, Abhinav Shukla, Richa Varshney, Prem Kalra, Subhashis Banerjee. *A grammar-based GUI for single view reconstruction*. ICVGIP 2012: 14.
28. Suvam Patra, Brojeshwar Bhowmick, Subhashis Banerjee, Prem Kalra. *High Resolution Point Cloud Generation from Kinect and HD Cameras using Graph Cut*. VISAPP (2) 2012: 311-316.
29. Abhishek Gupta, Jatin Kumar, Daniel J. Mathew, Sorav Bansal, Subhashis Banerjee, Huzur Saran. *Design and Implementation of the Workflow of an Academic Cloud*. DNIS 2011: 16-25.
30. Tanveer A. Faruque, Subhashis Banerjee, Prem K. Kalra. *Unsupervised discovery of activity correlations using latent topic models*. Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2010). December, 2010.
31. Ayesha Choudhary, Santanu Chaudhury, Subhashis Banerjee. *Distributed framework for composite event recognition in a calibrated pan-tilt camera network*. ICVGIP 2010: 140-147.
32. Chetan Arora, Subhashis Banerjee, Prem Kalra and S. N. Maheshwari. *An Efficient Graph Cut Algorithm for Computer Vision Problems*. European Conference on Computer Vision (ECCV 2010). pp. 552-565, September, 2010.
33. Tanveer Faruque, Prem Kalra and Subhashis Banerjee. *Time based Activity Inference using Latent Dirichlet Allocation*. British Machine Vision Conference (BMVC). September, 2009.
34. Ayesha Choudhary, Santanu Chaudhury, Subhashis Banerjee. *A Framework for Analysis of Surveillance Videos*. Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2008). December, 2008.
35. Ayesha Choudhary, Manish Pal, Subhashis Banerjee, Santanu Chaudhury. *Unusual Activity Analysis using Video Epitomes and pLSA*. Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2008). December, 2008.
36. Uma Mudanagudi, Subhashis Banerjee, Prem Kalra. *On improving space-time super resolution using a small set of video inputs*. Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2008). December, 2008.
37. Uma Mudanagudi, Ankit Gupta, Lakshya Goel, Avanish Kushal, Prem Kalra, and Subhashis Banerjee. *Super Resolution of images of 3D scenes*. ACCV 2007, Tokyo, Japan. Nov. 18-22, 2007. November, 2007.

363

Subhashis Banerjee: BIO-DATA

11

38. Ayesha Choudhary, Santanu Chaudhury, Subhashis Banerjee. *Unusual Activity Analysis in Video Sequences*. RSFDGrC 2007, LNCS 4482. pp. 443-450, August, 2007.
39. Subhajit Sanyal, Prem Kalra and Subhashis Banerjee. *Designing Quality Walkthroughs*. Computer Animation and Social Agents. (CASA 2007), Hasselt University, Belgium, June 2007.
40. Parag Chaudhuri, Prem Kalra and Subhashis Banerjee. *Reusing View-Dependent Animation*. Computer Graphics International (CGI 2007), Petropolis, Brazil, May 2007.
41. Uma Mudenagudi, Ram Singla, Prem Kalra and Subhashis Banerjee. *Super-resolution using Graph Cut*. ACCV 2006, LNCS 3852. pp. 385-394, January, 2006.
42. Ankit Mathur, Mayank Agarwal, Soumyadeb Mitra, Anup Gangwar, M. Balakrishnan, and Subhashis Banerjee. *SMPS: An FPGA-based Prototyping Environment for Multiprocessor Embedded Systems*. IEEE/ACM International Symposium on Field-Programmable Gate Arrays (FPGA 2005), Monterey, California. February, 2005.
43. Parag Chaudhuri, Ashwani Jindal, Prem Kalra and Subhashis Banerjee. *Stylistic Reuse of View-Dependent Animations*. Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2004). December, 2004.
44. Subhajit Sanyal, Mayank Bansal, Prem Kalra and Subhashis Banerjee. *On Learning Shapes from Shades*. Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2004). December, 2004.
45. Dhruv Mahajan, Nipun Kwatra, Sumit Jain, Prem Kalra and Subhashis Banerjee. *A Framework for Activity Recognition and Detection of Unusual Activities*. Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2004). December, 2004.
46. N. Gupta, P. Mittal, K. S. Patwardhan, S. Dutta Roy, S. Chaudhury, and S. Banerjee. *On-line Predictive Appearance-based Tracking*. IEEE International Conference on Image Processing (ICIP), Singapore. October, 2004.
47. Subhajit Sanyal, Mayank Bansal, Subhashis Banerjee, and Prem K Kalra. *Modeling of Free-Form Surfaces and Shape from Shading*. 2nd International Symposium on 3D Data Processing, Visualization, and Transmission 3DPVT'04, Thessaloniki, Greece. September, 2004.
48. Akash M Kushal, Gaurav Chanda, Kamishika Shrivastava, Mohit Gupta, Subhajit Sanyal, T.V.N. Sri Ram, Prem Kalra and Subhashis Banerjee. *Multilevel modelling and rendering of architectural scenes*. Eurographics, Granada (Spain). September, 2003.
49. Namita Gupta, Pooja Mittal, Sumantra Dutta Roy, Santanu Chaudhury, Subhashis Banerjee. *CONDENSATION-based Predictive EigenTracking*. Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP2002). December, 2002.
50. Puneet Sharma, Angshuman Parashar, Subhashis Banerjee and Prem Kalra. *An Uncalibrated Lightfield Acquisition System*. Indian Conference on Vision, Graphics and Image Processing (ICVGIP2002). December, 2002.

364

Subhashis Banerjee: BIO-DATA

'12

51. Akash M Kushal, Vikas Bansal and Subhashis Banerjee. *A simple method for interactive 3D reconstruction and camera calibration from a single view*. Indian Conference on Vision, Graphics and Image Processing (ICVGIP2002). December, 2002.
52. Gaurav Agarwal, Dinesh Rathi, Prem Kalra and Subhashis Banerjee. *A System for Image Based Rendering of Walk-Throughs*. Computer Graphics International (CGI2002), Bradford, UK. July, 2002.
53. N. Gupta, P. Mittal, S. Dutta Roy, S. Chaudhury, S. Banerjee. *A Predictive Scheme for Appearance-based Hand Tracking*. Proc. National Conference on Communications (NCC). pp. 513 - 522, January, 2002.
54. Sumantra Dutta Roy, Santanu Chaudhury and Subhashis Banerjee. *Recognizing Large 3-D Objects through Next View Planning using an Uncalibrated Camera*. IEEE International Conference on Computer Vision (ICCV). Vancouver, BC, Canada. pp. II: 276-281. July, 2001.
55. Shoma Chatterjee, Subhashis Banerjee and K. K. Biswas. *View Morphing based Facial Video Compression*. Proc. Indian Conference on Computer Vision, Graphics and Image-Processing (ICVGIP'2000), Bangalore, India. December, 2000.
56. Sumantra Dutta Roy, Santanu Chaudhury and Subhashis Banerjee. *Part-based Isolated 3-D Object Recognition through Next View Planning using Inner Camera Invariants*. Proc. Indian Conference on Computer Vision, Graphics and ImageProcessing (ICVGIP'2000), Bangalore, India. December, 2000.
57. Shoma Chatterjee, Subhashis Banerjee and K. K. Biswas. *Reconstruction of Local Features for Facial Video Compression*. IEEE ICIP'2000, Vancouver, BC, Canada. pp. TA07.02, September, 2000.
58. Michael Werman, Subhashis Banerjee, Sumantra Dutta Roy and Maolin Qiu. *Robot Localization using Uncalibrated Camera Invariants*. IEEE Conf. Computer Vision and Pattern Recognition (CVPR'99), Fort Collins, Colorado. pp. II:353-359. June, 1999.

365

Subrata Rakshit

Associate Director (Technology) at Centre for Artificial Intelligence and Robotics (CAIR)

Summary

R&D: Image Processing, Neural Networks, Multi-sensor data fusion, Computer Vision, Net Centric Operations

Management: Mentoring scientists and project managers, strategy formulation, R&D leadership

Experience

Associate Director (Technology)

September 2017 - Present

Scientist H / Outstanding Scientist

August 2017 - Present

R&D Leadership and Guidance

Scientist

December 1994 - Present

Scientists

1994 - Present

Analysis, Problem solving, Guidance

Sc G & Technical Mentor, Secure Systems Division

July 2014 - July 2017 (3 years 1 month)

Dream job in real life

Division Head, Secure Systems Division

January 2013 - June 2014 (1 year 6 months)

Goal setting, coordination between project teams, administrative functions, technical guidance

Group Head, Computer Vision

January 2000 - December 2012 (13 years)

Scientist, Neural Networks Group

December 1994 - December 1999 (5 years 1 month)

ANN classifier designs, Info Theory and Img Proc

Postdoc at Washington University at St. Louis

January 1994 - August 1994 (8 months)

Postdoc in field of image processing and computational neuroscience

366

Education

Caltech

PhD, Image Processing, 1988 - 1994

Indian Institute of Technology, Bombay

1984 - 1988

Indian Institute of Technology, Bombay

Bachelor of Technology - BTech, Engineering Physics, 1984 - 1988

Activities and Societies: Volleyball, bridge, dumb charades

La Martinierre for Boys, Kolkata

ISC Science, 1982 - 1984

Little Flower School

ICSE, English, Hindi, Maths, Science, Social Studies, 1970 - 1982

367

Y L P Rao

Deputy Director General at UIDAI, Government of India

Summary

N/A

Experience

Deputy Director General at UIDAI, Government of India

April 2013 - Present

Managing UIDAI Technology Division and Data Centers. Legal Issues. Supreme court and High court matters. Contract Management. Managing Contact Center Infrastructure and grievances through Contact Centers.

Chief Conservator of Forests

July 2011 - April 2013 (1 year 10 months)

Evaluation of All Developmental works executed by the Maharashtra State Forest Department.
Computerisation of Maharashtra State Forest Department including Geospatial Technology.

Conservator of Forests

June 1988 - July 2011 (23 years 2 months)

Visiting Faculty

2004 - 2009 (6 years)

Education

University of Pune

Ph.D - 2004 - 2007

Indian a Gandhi National Forest Academy, Dehradun

Indian Forest Service (I.F.S), Forestry, 1986 - 1988

University college of Engineering, Osmania University

B.E, Civil Engineering, 1980 - 1984

368

Annexure R-13

No. 10(36)/2015-EG-II (Vol-V)
 Government of India
 Ministry of Electronics & Information Technology
 e-Governance Group

Electronics Niketan,
 6, CGO Complex,
 Lodhi Road
 New Delhi - 110003
 Dated: 25.03.2017

Office Memorandum

Subject: Data Sharing - Compliance of the IT Act, 2000 and Aadhaar Act, 2016

It has come to notice that there have been instances wherein personal identity or information of residents, including Aadhaar number and demographic information, and other sensitive personal data such as bank account details etc. collected by various Ministries/Departments, State Government Departments, in the administration of its various welfare schemes etc. has been reportedly published online and is accessible through an easy online search.

The said act of publishing identity information i.e. Aadhaar number along with demographic information such as name, date of birth, address etc. is in clear contravention of the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, more specifically Section 29 (2), Section 29 (3) and 29 (4) and constitutes an offence under Sections 37, 40 & 41 punishable with imprisonment upto 3 years.

Further, publishing of financial information including bank account details, being sensitive personal data, is also in contravention of provisions under the Information Technology Act, 2000 and the Rules framed thereunder, more specifically Rule 3 & Rule 5 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 and constitutes an offence under Section 43 A of the Information Technology Act, 2000 and the offending parties are liable to pay damages by way of compensation to persons affected.

* In view of the above, it is hereby informed that any act of publishing personal identity or information i.e. Aadhaar number and demographic details alongwith personal sensitive information such as bank details, in contravention of the Aadhaar Act, 2016 and the Information Technology Act, 2000 may be refrained with immediate effect. Further, any such content already published and still appearing publicly may be discontinued with immediate effect.



Archana Dureja
 Scientist 'F'
 Phone: 011-24362528

To:

1. All Secretaries, Government of India
2. Chief Secretaries of all States/UTs
3. IT Secretaries of all States/UTs
4. Web Information Manager of websites (NIC)