

IN THE SUPREME COURT OF INDIA  
CIVIL APPELLATE JURISDICTION

Diary No. 14253 of 2019

SPECIAL LEAVE PETITION (CIVIL) NO. \_\_\_\_\_ OF 2019

IN THE MATTER OF:

S.G.VOMBATKERE AND ORS.

...PETITIONERS

VERSUS

UNION OF INDIA AND ORS.

...RESPONDENTS

DECLARATION

All defects have been duly cured. Whatever has been added/deleted/modified in the petition is the result of curing of defects and nothing else. Except curing the defects, nothing has been done. Paper books are complete in all respects.

(VIPIN NAIR)  
Advocate-On-Record  
Contact No. 9891061111

Date: 03.05.2019

**RECORD OF PROCEEDINGS**

**SR. NO.      RECORD OF PROCEEDINGS      PAGE NO.**

1.	Court's Order dated		
2.	Court's Order dated		
3.	Court's Order dated		
4.	Court's Order dated		
5.	Court's Order dated		
6.	Court's Order dated		
7.	Court's Order dated		
8.	Court's Order dated		
9.	Court's Order dated		
10.	Court's Order dated		
11.	Court's Order dated		
12.	Court's Order dated		
13.	Court's Order dated		
14.	Court's Order dated		
15.	Court's Order dated		
16.	Court's Order dated		
17.	Court's Order dated		
18.	Court's Order dated		
19.	Court's Order dated		
20.	Court's Order dated		
21.	Court's Order dated		

INDEX

Sl. NO.	Particulars of Document	Page No. of part to which it belongs		Remarks
		Part I (Contents of Paper Book)	Part II (Contents of file alone)	
(i)	(ii)	(iii)	(iv)	(v)
1.	O/R ON LIMITATION	A	A	
2.	LISTING PROFORMA	A1-A2	A1-A2	
3.	COVER PAGE OF PAPER BOOK		A-3	
4.	INDEX OF RECORD OF PROCEEDINGS		A-4	
5.	LIMITATION REPORT PREPARED BY THE REGISTRY		A-5	
6.	DEFECT LIST		A-6	
7.	NOTE SHEET			
8.	SYNOPSIS AND LIST OF DATES	B-P		
9.	WRIT PETITION WITH AFFIDAVIT	1-49		
10.	<u>APPENDIX</u> i) A COPY OF THE AADHAAR AND OTHER LAWS (AMENDMENT) ORDINANCE 2019.	50-61		
11.	<u>ANNEXURE P-1</u> A COPY OF THE RESUME OF THE 1ST PETITIONER'S S. G. VOMBATKERE	62		
12.	<u>ANNEXURE P-2</u> A COPY OF THE RESUME OF THE 2ND PETITIONER'S BEZWADA WILSON	63		
13.	<u>ANNEXURE P-3</u> COPY OF THE AADHAAR AND OTHER LAWS (AMENDMENT) ORDINANCE, 2019	64-75		
14.	<u>ANNEXURE P-4</u> TRUE COPY OF THE AADHAAR (PRICING OF AADHAAR AUTHENTICATION SERVICES) REGULATIONS, 2019	76-78		
15.	<u>ANNEXURE P-5</u> TRUE COPY OF THE AFFIDAVIT DR. SAMIR KELEKAR'S AFFIDAVIT DATED 2.4.2019 ALONG WITH A COPY OF HIS AFFIDAVIT DATED 6.4.2016	79-84		
16.	<u>ANNEXURE P-6</u> TRUE COPY OF THE AFFIDAVIT JUDE TERRENCE D'SOUZA'S AFFIDAVIT DATED 11.4.2019 ALONG WITH A COPY OF HIS AFFIDAVIT DATED 22.11.2016	85-95		
17.	<u>ANNEXURE P-7</u> TRUE COPY OF DR. MANINDRA AGRAWAL'S REPORT DATED 04.03.2018	96-102		
18.	<u>ANNEXURE P-8</u> TRUE COPY OF THE NEWSPAPER ARTICLES ENTITLED (I) "IT FIRM WORKING ON APP FOR TDP 'STOLE' DATA OF ANDHRA VOTERS, SAY COPS," SREENIVAS JANYALA, INDIAN EXPRESS DATED 05.03.2019	103-105		

19.	<u>ANNEXURE P-9</u> TRUE COPY OF THE NEWSPAPER ARTICLES ENTITLED (II) "TDP APP BREACHED DATA OF 3.7CR VOTERS? PROBE BEGINS," TIMES NEWS NETWORK DATED 26.02.2019	106-108		
20.	<u>ANNEXURE P-10</u> A COPY OF THE FIR DATED 02.03.2009 FILED BY ONE, THUMALLA LOKESWARA REDDY	109-112		
21.	<u>ANNEXURE P-11</u> TRUE COPY OF THE RELEVANT RBI CIRCULARS DATED 27.01.2011	113-116		
22.	<u>ANNEXURE P-12</u> TRUE COPY OF THE RELEVANT RBI CIRCULARS DATED 28.09.2011	117-119		
23.	<u>ANNEXURE P-13</u> TRUE COPY OF THE NEWSPAPER REPORTS ENTITLED "SBI ALLEGES AADHAAR DATA MISUSE, UIDAI RUBBISHES CHARGE," PUBLISHED IN THE TIMES OF INDIA DATED 29.01.2019	120-124		
24.	<u>ANNEXURE P-14</u> TRUE COPY OF THE NEWSPAPER REPORTS ENTITLED "AADHAAR DETAILS OF ENROLMENT OPERATOR STOLEN AND MISUSED, SHOW UIDAI RECORDS: REPORT," PUBLISHED IN SCROLL DATED 20.02.2019	125-126		
25.	APPLICATION FOR STAY	127-130		
26.	F/M	131		
27.	V/A	132-133		

A)

PROFORMA FOR FIRST LISTING

SECTION PIL

The case pertains to (Please tick/check the correct box):

Central Act : (Title) A COPY OF THE AADHAAR AND OTHER LAWS (AMENDMENT) ORDINANCE 2019

Section : \_\_\_\_\_ N/A \_\_\_\_\_

Central Rule : (Title) \_\_\_\_\_ NA \_\_\_\_\_

Rule No (s) : \_\_\_\_\_ N/A \_\_\_\_\_

State Act : (Title) \_\_\_\_\_ N/A \_\_\_\_\_

Section : \_\_\_\_\_ N/A \_\_\_\_\_

State Rule : (Title) \_\_\_\_\_ N/A \_\_\_\_\_

Rule No(s) : \_\_\_\_\_ N/A \_\_\_\_\_

Impugned Interim Order : (Date) \_\_\_\_\_ NA \_\_\_\_\_

Impugned Final Order/Decree : (Date) \_\_\_\_\_

High Court: (Name) \_\_\_\_\_

Names of Judges: CORAM: \_\_\_\_\_

Tribunal/Authority : (Name) \_\_\_\_\_ NA

1. Nature of Matter :  Civil  Criminal

(a) Petitioner/appellant No. 1 : S.G.VOMBATKERE AND ANOTHER

(b) E-mail ID : \_\_\_\_\_ N/A \_\_\_\_\_

(c) Mobile phone number : \_\_\_\_\_ N/A \_\_\_\_\_

3 (a) Respondent : UNION OF INDIA AND ANOTHER

(b) E-mail ID : \_\_\_\_\_ N/A \_\_\_\_\_

(c) Mobile phone number : \_\_\_\_\_ N/A \_\_\_\_\_

4. (a) Main category classification : \_\_\_\_\_

(b) Sub classification : \_\_\_\_\_

A-2

5. Not to be listed before : \_\_\_\_\_ N/A \_\_\_\_\_
6. Similar/Pending matter : \_\_\_\_\_ N/A \_\_\_\_\_
7. Criminal Matters :
- (a) Whether accused/convict has surrendered:  Yes  No
- (b) FIR No.                      Date : NA
- (c) Police Station:                      NA
- (d) Sentence Awarded :                      NA
- (e) Sentence Undergone :                      NA
8. Land Acquisition Matters:
- (a) Date of Section 4 notifications : \_\_\_\_\_ N/A \_\_\_\_\_
- (b) Date of Section 6 notifications : \_\_\_\_\_ N/A \_\_\_\_\_
- (c) Date of Section 17 notifications: \_\_\_\_\_ N/A \_\_\_\_\_
9. Tax Matters : State the tax effect : \_\_\_\_\_ N/A \_\_\_\_\_
10. Special Category (first petitioner/appellant only): N/A
- Senior citizen >65 years       SC/ST       Woman/child
- Disabled       Legal Aid case       In custody
11. Vehicle Number (in case of Motor Accident Claim matters): N/A
12. Decided cases with citation : \_\_\_\_\_ N/A \_\_\_\_\_

NEW DELHI  
FILED ON: -16.04.2019

VIPIN NAIR  
ADVOCATE-ON-RECORD  
FOR THE PETITIONER(S)  
nairvipin73@gmail.com  
Registration No. 1295

SYNOPSIS

- A. The present writ petition under Article 32 of the Constitution of India is being filed in public interest to challenge the *Aadhaar and Other Laws (Amendment) Ordinance, 2019* ("the impugned Ordinance") and the *Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019* ("the impugned Regulations,") on the grounds that, inter alia, that they violate the fundamental rights as guaranteed under Part III of the Constitution of India. The impugned Ordinance creates a backdoor to permit private parties to access the Aadhaar eco-system, thus enabling State and private surveillance of citizens, and the impugned Regulations permit the commercial exploitation of personal and sensitive information which has been collected and stored for State purposes only.
- B. First, the impugned Ordinance and Regulations are manifestly unconstitutional as they seek to re-legislate the provisions of the Aadhaar Act, 2016 which enabled commercial exploitation of personal information collected for the purposes of the state (by permitting private parties to access the Aadhaar database,) which were specifically declared unconstitutional in the "Aadhaar case," titled *Justice Puttuswamy (Retd.) vs. Union of India & Anr.*, reported at 2019 1 SCC 1. In that judgement, this Hon'ble Court found that architecture and design of the Aadhaar project did not enable mass surveillance of persons enrolled under the Aadhaar Act, only after striking down certain offending provisions, including Section 57 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, which permitted private parties to use Aadhaar for authentication, and limiting its use to only two uses, and only by the government.

C. Second, the Aadhaar database lacks integrity as it has no value other than, at most, the underlying documents on the basis of which the Aadhaar numbers are issued. As admitted before this Hon'ble Court, none of the data uploaded at the time of enrolment is verified by anyone, much less a government official. Permitting such a database to be linked with the existing databases of services offered under Chapter IV of the Prevention of Money Laundering Act, 2002, and Section 4 of the Indian Telegraph Act, 1885, poses a grave threat to national security by permitting unverified data to creep into these databases. The Aadhaar database is a Trojan Horse which will over time infect, undermine and debase the integrity of these two databases. The purported utilization of the same for e-KYC and verification of identity for the use of services is manifestly arbitrary and compromises national security and the integrity of the financial system of the country.

3. Third, the impugned Ordinance creates a new system of "offline verification," that purports to bypass the Respondent Authority. However, this method exacerbates the problems caused by the Aadhaar project, as such a method creates unprecedented opportunities for unauthorized parties to save and replicate Aadhaar-related personal data, in various offline federated databases. These databases are themselves impermissible under the Aadhaar Act, and unconstitutional inasmuch as they enable private entities to store and commercialise citizens' personal data.

D

- E. Third, through the impugned Regulations, the UIDAI expressly seeks to commercialise, and gain financially through the large-scale collection of the citizen's private data and the use of Aadhaar database by private entities. Peoples' data, which was collected for the Aadhaar database, is their private property and permitting this to be commercialised is an impermissible violation of their dignity under Article 19 and 21 of the Constitution of India.
- F. Finally, the Ordinance was promulgated in an improper exercise of the Ordinance-making powers of the President under Article 123 of the Constitution of India.
- G. Unless the reliefs sought here are granted, the impugned Ordinance and Regulations will result in creating a surveillance state and will enable the Aadhaar database to be exploited by private players for commercial gain.

LIST OF DATES

- 28.01.2009      The Union of India through the Planning Commission issued a Notification dated 28.01.2009, constituted the Unique Identification Authority of India (UIDAI) for the purpose of implementing of Unique Identity (UID) scheme wherein a UID data base was to be collected from the residents of India. Notably, there was no mention of collection of biometric information in the said notification. Furthermore the notification did not provide any checks and balance with

E

regard to the collection, storage, usage of the said information collected pursuant to the UID scheme.

03.12.2010 Although the programme was launched in September 2010, there was no statutory backing for the same. On 03.12.2010, the Union of India introduced the National Identification Authority of India Bill 2010 (NIA Bill) in Parliament. The NIA Bill was almost identical in pith and substance to the Aadhaar Act, 2016.

30.11.2012 Aggrieved by the violation of fundamental rights of the citizens of India, several PILs were filed before this Hon'ble Court. The lead petition before this Hon'ble Court was *Justice K. S. Puttaswamy (Retd) v. Union of India & Ors.*, W.P. (C) No.494/2012. This Hon'ble Court vide Order dated 30.11.2012 issued notice in the said petition.

3.09.2013 The Petitioners herein filed a writ petition, viz. W.P. (C) No. 829/2013, titled 'S.G. Vombatkere and Anr. vs. Union of India & Anr.'.

A 2-Judge Bench vide Order dated 23.09.2013, while issuing notice in the Review Petitioners' writ petition, stated,

*"All the matters require to be heard finally. List all matters for final hearing after the Constitution Bench is over.*

*In the meanwhile, no person should suffer for not getting the Aadhaar card inspite of the fact that some*

*authority had issued a circular making it mandatory and when any person applies to get the Adhaar Card voluntarily, it may be checked whether that person is entitled for it under the law and it should not be given to any illegal immigrant."*

26.11.2013 A 2-Judge Bench vide Order dated 26.11.2013, held,

*"After hearing the matter at length, we are of the view that all the States and Union Territories have to be impleaded as respondents to give effective directions. In view thereof notice be issued to all the States and Union Territories through standing counsel.*

...

*Interim order to continue, in the meantime."*

24.03.2014 In UIDAI's own SLP (CrI) No. 2524/2014 assailing a Bombay High Court order requiring UIDAI to disclose biometric details of an accused, a 2-Judge Bench vide Order dated 24.03.2014 directed,

*"In the meanwhile, the present petitioner is restrained from transferring any biometric information of any person who has been allotted the Aadhaar number to any other agency without his consent in writing.*

*More so, no person shall be deprived of any service for want of Aadhaar number in case he/she is otherwise eligible/entitled. All the authorities are directed to modify their forms/circulars/likes so as to not compulsorily require the Aadhaar number in order to meet the requirement of the interim order*

*passed by this Court forthwith."*

16.03.2015 A 3-Judge Bench vide Order dated 16.03.2015, stated,

*"In the meanwhile, it is brought to our notice that in certain quarters, Aadhar identification is being insisted upon by the various authorities, we do not propose to go into the specific instances.*

*Since Union of India is represented by learned Solicitor General and all the States are represented through their respective counsel, we expect that both the Union of India and States and all their functionaries should adhere to the Order passed by this Court on 23rd September, 2013."*

11.08.2015 A 3-Judge Bench vide Order dated 11.08.2015, while referring the matter to larger bench to decide the issue whether privacy is a fundamental right, passed the following interim order,

*"Having considered the matter, we are of the view that the balance of interest would be best served, till the matter is finally decided by a larger Bench if the Union of India or the UIDA proceed in the following manner:-*

- 1. The Union of India shall give wide publicity in the electronic and print media including radio and television networks that it is not mandatory for a citizen to obtain an Aadhaar card;*
- 2. The production of an Aadhaar card will not be condition for obtaining any benefits otherwise due*

*to a citizen;*

*3. The Unique Identification Number or the Aadhaar card will not be used by the respondents for any purpose other than the PDS Scheme and in particular for the purpose of distribution of foodgrains, etc. and cooking fuel, such as kerosene. The Aadhaar card may also be used for the purpose of the LPG Distribution Scheme;*

*4. The information about an individual obtained by the Unique Identification Authority of India while issuing an Aadhaar card shall not be used for any other purpose, save as above, except as may be directed by a Court for the purpose of criminal investigation."*

15.10.2015

A Constitution Bench vide Order dated 15.10.2015, while partly modifying the aforesaid interim order, passed the following order,

*"3. After hearing the learned Attorney General for India and other learned senior counsels, we are of the view that in paragraph 3 of the Order dated 11.08.2015, if we add, apart from the other two Schemes, namely, P.D.S. Scheme and the L.P.G. Distribution Scheme, the Schemes like The Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), National Social Assistance Programme (Old Age Pensions, Widow Pensions, Disability Pensions) Prime Minister's Jan Dhan Yojana (PMJDY) and Employees' Provident Fund Organisation (EPFO) for the present, it would not dilute earlier order passed by this Court. Therefore, we now include the aforesaid Schemes apart from the other two Schemes that this Court has permitted*

*in its earlier order dated 11.08.2015.*

*4. We impress upon the Union of India that it shall strictly follow all the earlier orders passed by this Court commencing from 23.09.2013.*

*5. We will also make it clear that the Aadhaar card Scheme is purely voluntary and it cannot be made mandatory till the matter is finally decided by this Court one way or the other."*

16.3.2016

In the above backdrop, the Union of India, introduced the Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016 (impugned Aadhaar Act) as a Money Bill in the Budget Session, 2016 in the Lok Sabha.

The Aadhaar Act was in pith and substance identical to the earlier NIA Bill, 2009.

In spite of objections with regard to the impugned Aadhaar Act being introduced as a Money Bill, the same came to be passed on 16.3.2016.

26.3.2016

The impugned Act received Presidential assent and was published in the official gazette on 26.3.2016.

12.7.2016

Vide Notification dated 12.7.2016 certain provisions of the impugned Act were brought into force w.e.f. 12.7.2016.

The Union of India vide Notification dated 12.7.2016 issued under Section 11 of the Impugned Act,

established the 2nd Respondent/UIDAI.

12.9.2016 Vide Notification dated 12.9.2016, the remaining provisions of the impugned Act was brought into force. Section 7 of the impugned Act was brought into force by this Notification.

28.10.2016 A number of PILs were filed before this Hon'ble Court challenging the impugned Act. The first writ petition challenging the impugned Act is WP No. 797/2016 titled 'S.G. Vombatkere and Anr. vs. Union of India & Anr.'. This Hon'ble Court vide Order dated 28.10.2016, issued rule nisi, and tagged the matter with the above-mentioned petitions, which were pending adjudication before the Constitution Bench.

January 2017 The Respondent No. 1, through its different Ministries, issued various Notifications under Section 7 of the impugned Act, making the Aadhaar number a mandatory requirement for an individual to avail different benefits, services and subsidies.

6.02.2017 In spite the specific direction by this Court to not use the Aadhaar platform, TRAI launched the Aadhaar based e-KYC for mobile connections.

The Respondent No. 1/Union of India in a separate proceeding before this Hon'ble Court, has sworn on affidavit that they are using the Aadhaar platform for

verification of sim cards. This Hon'ble Court vide Order dated 6.2.2017 in the matter of '*Lokniti Foundation v. Union of India and Anr.*, WP No. 607/2016', has taken note of the same.

31.3.2017 The Union of India introduced Section 139AA of the Income Tax Act, 1961 (by way of Section 56 of the Finance Act, 2017) making it mandatory to present an Aadhaar number for the following: - (a) obtaining a permanent account number ("PAN"); (b) continued validity of a person's PAN; and (c) filing one's return of income under the Income Tax Act.

23.03.2017 The Department of Telecommunication vide Impugned Circular dated 23.03.2017 directed all mobile companies to carry out re-verification of existing customers (both postpaid and prepaid) by carrying out e-KYC, which requires the customer to provide his or her Aadhaar number on or before 8.02.2018.

01.06.2017 Prevention of Money Laundering (Maintenance of Records) Second Amendment Rules, 2017 was passed by the Union of India making the Aadhaar number mandatory for e-KYC. Consequently, Aadhaar is mandatory for opening and maintaining of bank account, for carrying out any financial transaction equal to or exceeding Rs. 50,000/-, holding investments in mutual

funds and holding insurance policies.

09.06.2017 A 2-Judge Bench of this Hon'ble Court vide Judgment dated 9.06.2017 in the matter titled '*Binoy Viswam v. Union of India & Ors.*', Writ Petition (Civil) No. 247 of 2017, upheld the validity of Section 139AA of the Income Tax Act, under Articles 14 and 19.

It directed that those who have already enrolled themselves under Aadhaar scheme would comply with the requirement of sub-section (2) of Section 139AA of the Income Tax Act. Those who still want to enrol are free to do so. However, the PAN cards of those who are not Aadhaar card holders, and do not comply with the provision of Section 139(2), can be not treated as invalid for the time being.

24.08.2017 A 9-Judge Constitution Bench of this Court vide Judgment dated 24.08.2017 in WP No. 494/2012 titled '*Justice K.S. Puttaswamy (retd) & Anr vs. Union of India & Ors.*' along with other matters, decided the 'referred issue' relating to the existence of the fundamental right to privacy.

This Court unanimously held that there exists a fundamental right to privacy and remitted the matter back for adjudication.

27.01.2011 Reserve Bank of India ("RBI") issued Circular No.

M

RBI/2010-11/389 directing bank accounts opened exclusively on the basis of Aadhaar letter to be treated as "small accounts".

28.09.2011

RBI issues Circular No. RBI/2011-12/207 directing all Scheduled Commercial Banks/ All India Financial Institutions to accept Aadhaar as an officially valid document, and further directing banks to verify the residential addresses of persons for accounts being opened on the basis of an Aadhaar number through additional means.

26.09.2018

A five-judge bench of this Hon'ble Court passed its final order and judgement, disposing of the batch of writ petitions filed under Article 32 of the Constitution vide judgement dated 26.09.2018 titled *Justice K.S. Puttaswamy (Retd.) And Another vs. Union Of India &Ors.* in W.P. No. 494 of 2012. The Judgement was given by Justice A.K. Sikri, writing for himself, Chief Justice Dipak Misra and Justice Khanwilkar, Justice Bhushan who broadly concurred with the majority judgement, and Justice D.Y. Chandrachud, writing in dissent. This Hon'ble Court upheld only two uses of the Aadhaar database, and only by the government. It also ruled that even voluntary use of the Aadhaar database for authentication by private parties was unconstitutional. The Hon'ble Court also noted the importance of bringing

N

in a Data Protection Bill as per the recommendations of the Srikrishna Committee.

03.01.2019 In the case titled *DebashisNandy v. Union of India*, (W.P. 15233 (W) of 2018), a Single Judge of the Calcutta High Court noted that there was no verification of the authenticity of the demographic data in the Aadhaar database.

04.01.2019 The Aadhaar and Other Laws (Amendment) Bill, 2018 was passed in Lok Sabha.

09.01.2019 In a case titled *Smt. Parvati Kumar v. State of U.P.* (Misc. Bench No. 13419 of 2018), a Division Bench of the Lucknow Bench of the Allahabad High Court held that the information entered in the Aadhaar card cannot be treated as conclusive proof of the same as it is unverified by any party.

13.02.2019 While the *Aadhaar and Other Laws (Amendment) Bill, 2019* was pending before the Rajya Sabha, the Lok Sabha dissolved. The Bill lapsed.

29.01.2019 An article entitled "*SBI alleges Aadhaar data misuse, UIDAI rubbishes charge*," was published in the TIMES OF INDIA, which reported that State Bank of India ("**SBI**") was penalized for failing to meet the enrolment targets set by the UIDAI, because many of the vendors appointed by SBI had been deactivated or blacklisted for unauthorized enrolments. SBI alleged that the enrollment details of their

0

vendors had been stolen and misused. The Response Authority UIDAI denied that this breach had taken place.

20.02.2019 An article entitled "*Aadhaar details of enrolment operator stolen and misused, show UIDAI records: Report,*" was published in SCROLL, reporting that the biometrics of an enrolment official who was a vendor with the State Bank of India in Chandigarh, had been stolen, and used to generate false enrolments under Aadhaar enrolments. This official had been previously penalised Rs. 33 lakh by the UIDAI for alleged fraudulent transactions.

26.02.2019 An article entitled "*Andhra Pradesh: TDP app breached data of 3.7 crore voters? Probe begins,*" was published in the TIMES OF INDIA, which reported allegations of misuse of the demographic data collected during Aadhaar enrolment of more than 3.7 crore voters in Andhra Pradesh.

02.03.2019 The impugned "**Aadhaar and Other Laws (Amendment) Ordinance, 2019,**" was promulgated by the President of India. This was materially same as the Aadhaar Amendment Bill, which had lapsed.

02.03.2009 An FIR filed by oneThumallaLokeswara Reddy, under Sections 66-B and 72 of the Information Technology Act, 2000 and Sections 120b, 379, 420 and 188 of the Indian Penal Code alleges vast misuse of demographic data,

P

including Aadhaar data for private and election related purposes.

05.03.2019 An article entitled "IT Firm working on app for TDP 'stole' data of Andhra voters, say cops," was published in the INDIAN EXPRESS, reported that Aadhaar related data amongst other data, had been stolen and misused for private and election related purposes.

7.03.2019 The impugned "Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019" were notified by the UIDAI, under which the UIDAI will charge private entities Rs. 20 per e-KYC transaction, and Rs.0.50 per Yes/No authentication transaction.

16.04.2019 Hence this present petition.

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. \_\_\_\_\_ OF 2019

(UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA)

BETWEEN

1. S. G. VOMBATKERE, INDIAN  
INHABITANT HAVING HIS  
ADDRESS AT 475, 7TH MAIN ROAD,  
VIJAY NAGAR 1<sup>ST</sup> STAGE,  
MYSORE, KARNATAKA -570 017.

2. BEZWADA WILSON C/O  
SAFAIKARMACHARIANDOLAN,  
36/13, GROUND FLOOR, EAST  
PATEL NAGAR, NEW DELHI -  
110008.

...PETITIONERS

VERSUS

1. UNION OF INDIA, THROUGH THE  
SECRETARY, MINISTRY OF  
FINANCE, NORTH BLOCK, NEW  
DELHI-110001.

2. UNIQUE IDENTIFICATION  
AUTHORITY OF INDIA A  
STATUTORY AUTHORITY  
ESTABLISHED UNDER THE  
AADHAAR (TARGETED DELIVERY  
OF FINANCIAL AND OTHER  
SUBSIDIES, BENEFITS AND  
SERVICES) ACT, 2016 HAVING ITS  
ADDRESS AT 3<sup>RD</sup> FLOOR, TOWER-  
II, JEEVAN BHARATI BUILDING,  
CONNAUGHT CIRCUS, NEW  
DELHI-110001.

... RESPONDENTS

WRIT PETITION UNDER ARTICLE 32 OF  
THE CONSTITUTION OF INDIA

TO  
THE HON'BLE THE CHIEF JUSTICE  
OF INDIA AND HIS OTHER  
COMPANION JUSTICES OF THE  
HON'BLE THE SUPREME COURT OF  
INDIA.

THE HUMBLE PETITION OF THE  
PETITIONERS ABOVENAMED

MOST RESPECTFULLY SHOWETH:

A. PARTIES

The Petitioners

1 (a). "This Writ Petition has been preferred in public interest seeking inter alia an appropriate writ, order or direction in the nature of a mandamus to declare the Aadhaar and Other Laws (Amendment) Ordinance, 2019 as ultra vires, unconstitutional, null and void and in particular violative of Articles 14, 19 and 21 of the Constitution of India." The 1<sup>st</sup> petitioner, a citizen of India, is aged about 77 years. The 1<sup>st</sup> petitioner is a retired Indian Army officer and is engaged in voluntary social work. In so far as the Unique Identification Project ("**UID project**") is concerned, the 1<sup>st</sup> petitioner has published several articles expressing concerns over privacy and security risks. The Petitioner has no Civil, criminal or revenue litigation involving the Petition, which could have a legal nexus with the issues involved in the present Writ Petition (PIL). The Petitioner has no personal or private interest in the matter. The PAN Number of the Petitioner is ABMPV3365Q. The Petitioner's annual income in last AY is Rs. Rs. 14,83,000/- (approx ) Petitioner Email is [sq9kere@live.com](mailto:sq9kere@live.com) – and Mob. 94804 75925. A resume of the 1<sup>st</sup> petitioner's professional work is annexed hereto and marked as **ANNEXURE P-1 at page 62** .

1(b). The 2<sup>nd</sup> petitioner is a citizen of India and is also engaged in voluntary social work. He is a human rights activist. He is one of the founders and the National Convenor of the Safai Karmachari Andolan, a human rights organization that has been campaigning for the eradication of manual scavenging and the emancipation of people employed for the purposes of manual scavenging. He was also the convenor of the sub-group on safai karamcharis constituted by the Planning Commission of India. In 2009, he was chosen as the "Ashoka Senior Fellow" of human rights. In 2016 he was conferred the Raman

Magsaysay Award. By virtue of being the founder of Safai Karmachari Andolan, he is also actively involved in a public interest litigation pending before this Hon'ble Court in Writ Petition (Civil) No. 583 of 2003, *Safai Karamchari Andolan and Ors v. Union of India & Ors*. The subject matter of that petition is strict implementation of the Employment of Manual Scavengers and Construction of Dry Latrines (Prohibition) Act, 1993. The Petitioner has no Civil, criminal or revenue litigation involving the Petition, which could have a legal nexus with the issues involved in the present Writ Petition (PIL). The Petitioner has no personal or private interest in the matter. The PAN Number of the Petitioner is AGMPB6495N. The Petitioner's annual income in last AY is Rs. 11,46,000/- (approx) Petitioner Email is [skandolan@gmail.com](mailto:skandolan@gmail.com) – and Mob. 9311234783. A resume of the 2<sup>nd</sup> petitioner's professional work is annexed hereto and marked as **ANNEXURE P-2 at pages 63.**

- 1(c). The petitioners herein filed Civil Writ Petition No. 829 of 2013 (*S.G. Vombatkere & Anr. v. Union of India & Ors*) relating to the Aadhaar project before the enactment of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. They also filed Civil Writ Petition No. 797 of 2016 (*S.G. Vombatkere & Anr. v. Union of India & Ors*) challenging the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. The final judgment and order in Writ Petition No.829 of 2013 and 797 of 2016 was delivered on 26.09.2018.
- 1(d). The Petitioners have filed a review petition bearing No. 924/19 in respect of the judgment delivered on 26.09.2018. The review petition is pending. The review petition seeks review of the majority judgments rendered in that case. The submissions set forth in this petition are strictly without prejudice to what is set out in the review petition.

1(e). Neither of the petitioners have an Aadhaar number.

The Respondents

2(a). The 1<sup>st</sup> Respondent is the Union of India.

2(b). The 2<sup>nd</sup> Respondent is the Unique Identification Authority of India (UIDAI), a statutory authority established under Section 11 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("**Aadhaar Act**"). It was initially established under an executive notification dated 28.01.2009 and thereafter brought under the 2016 statute.

3. The Respondents are amenable to the writ jurisdiction of this Hon'ble Court under Article 32 of the Constitution of India. The Respondents are "State" within the meaning of Article 12 of the Constitution of India.

**B. PUBLIC INTEREST LITIGATION**

4. This petition is filed as a public interest litigation to challenge the Aadhaar and Other Laws Amendment Ordinance, 2019 ("**impugned Ordinance**") and the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 ("**impugned Regulations**").

5. The Petitioners are preferring this petition in general public interest, as they fear the deleterious impact that the impugned Ordinance and Regulations will have on fundamental rights of citizens guaranteed under Part III of the Constitution, and for the security of personal data, which is imperiled by allowing private players access to it. Furthermore, due to the deeply flawed enrollment system to create the Aadhaar database, the information available with the 2<sup>nd</sup> Respondent is unverified by any government agency and lacks integrity. The purported utilization of the same for e-KYC and verification of identity for the use of services is manifestly arbitrary and compromises national security and the integrity of the financial system of the country.

6. The impugned Ordinance, unless set aside as being *ultra vires* the Constitution of India, will adversely affect and harm citizens across the country, individually and collectively. The Petitioners approach this Hon'ble Court *bona fide* to prevent the violation of basic human rights that has already occurred as a result of the UID project, and the lack of implementation of the Judgment dated 26.09.2018 of this Court in the case of *Justice Puttuswamy(Retd.) v. Union of India &Anr.* W.P. (Civil) 494 of 2012 & related matters reported at (2019) 1 SCC 1 ("**Aadhaar judgment**"). Unless the reliefs sought here are granted, the impugned Ordinance will result in the creation of a surveillance state and the Aadhaar database will be exploited by private players for commercial gain. Moreover, the impugned Ordinance will severely imperil national security and the financial integrity of the country. The Aadhaar judgment sought to protect the citizenry from these threats and the impugned Ordinance seeks to illegally resurrect and restore the programme that was drastically curtailed by this Hon'ble Court.
7. The Petitioners have not filed any other petition challenging the impugned Ordinance, either in this Hon'ble Court or in any High Court.

**C. ANALYSIS OF THE AADHAAR JUDGMENT (2019) 1 SCC 1**

8. This analysis is restricted to the issues relevant to this petition.
9. The 3 judgments were rendered by this Hon'ble Court on 26.09.2018 when deciding the constitutional validity of the Aadhaar Act. The principal majority judgment authored by Dr. A. K. Sikri, J. spoke for three Learned Judges. Broadly, Ashok Bhushan, J. concurred with the majority and found certain provisions that the majority held

unconstitutional to be valid. Dr. D. Y. Chandrachud, J. delivered a dissent and found the Aadhaar Act to be unconstitutional.

10. The Petitioners having taken legal advice believe that the view taken in the dissent is the correct view and it is for this reason that review petition was filed.
11. In the submissions made before the Constitution Bench in the challenge to the Aadhaar Act, the petitioners submitted that the architecture of Aadhaar was inherently flawed. The design of Aadhaar would result in surveillance of those authenticating. Coupled with the extensive mandatory use of Aadhaar which was being compelled on all citizens, the petitioners projected that the nation would transform into a surveillance society.
12. This submission was dealt with by adopting separate approaches. The dissenting judgment accepts the position with respect to the surveillance architecture and finding that this would amount to an intolerable incursion on a free society, strikes down the law.
13. The principal majority judgment while recording the submission, addresses the concerns obliquely, not directly. The principal majority judgment severely downsizes the project and contains its ambit. It does so by: (i) reading narrowly the expressions "subsidy, benefit or service"; (ii) excluding children from the scope of Aadhaar; (iii) excluding private sector companies from using Aadhaar for authentication; (iv) striking down actions by the government to make Aadhaar mandatory for cell phones; (v) striking down the requirement to link Aadhaar to every

bank account, etc. By containing Aadhaar and limiting it only to subsidies that could be linked to the Consolidated Fund of India, the principal majority judgment shrank the programme and thereby sought to address the problem of privacy violation.

14. Very significantly the principal majority judgment seeks to allay the serious concerns with respect to surveillance, by limiting authentication to those who avail subsidies, which in most cases might involve authentication once in a month.
15. The impugned Ordinance, by seeking to resurrect the programme and by seeking to expand it to cover "non-section 7" situations where no subsidy, benefit or service relatable to the Consolidated Fund of India is involved, is not only contrary to the principal majority judgment but also props up the discredited surveillance architecture.
16. Another test applied by the principal majority judgment to strike down the extension of Aadhaar beyond the subsidy, benefit and service category relatable to the Consolidated Fund of India was the proportionality test. The impugned ordinance by extending Aadhaar beyond section 7 of the Aadhaar Act *ex-facie* breaches the proportionality test laid down by this Hon'ble Court to protect the privacy of citizens.
17. Indeed, there are clear red lines laid down in the principal majority judgment. The first red line is that no private entity or corporation can use Aadhaar authentication for any purpose irrespective of whether such use is voluntary. A second red line with regard to privacy rights of

individuals is that Aadhaar cannot form a basis for commercial exploitation. Such commercial exploitation is barred both on the part of the State as well on the part of private entities. A third red line is that Aadhaar may be used only for limited designated purposes backed by statute and that too only by the State. It is respectfully submitted that the impugned Ordinance breaches these red lines laid down in the principal majority judgment for the protection of the fundamental rights of citizens of India including privacy rights.

#### **D. ISSUES INVOLVED IN THE PRESENT PETITION**

18. This petition challenges the Aadhaar and Other Laws Amendment Ordinance, 2019 inasmuch as it violates and threatens to violate the fundamental rights of the Petitioners and other citizens of India. The impugned Ordinance, in particular, violates the fundamental rights guaranteed under Articles 14, 19 and 21 of the Constitution of India. It also contravenes the final order and judgment of the Supreme Court of India in the "Aadhaar case".
19. The Petitioners seek appropriate declarations to the effect that the impugned Ordinance is *ultra vires* the Constitution of India. Should this Court uphold the validity of the impugned Ordinance, the petitioners urge an alternative case that key portions of the impugned Ordinance are *ultra vires* the Constitution of India and seek appropriate declarations with respect to the unconstitutionality of those particular provisions.
20. The impugned Ordinance was published in the Gazette of India on 2<sup>nd</sup> March 2019. A copy of the Aadhaar and other Laws (Amendment)

Ordinance, 2019 is annexed and marked as **ANNEXURE P-3 at pages 64 to 75.**

21. This petition also challenges the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 as being violative of the fundamental rights of privacy and property and seeks appropriate directions in relation to these regulations. The impugned Ordinance was published in the Gazette of India on 6<sup>th</sup> March 2019. A copy of the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 is annexed and marked as **ANNEXURE P-4 at pages 76 to 78.**

#### **E. BRIEF FACTS**

22. The Union of India, through the Planning Commission issued a Notification dated 28.01.2009, constituting the Unique Identification Authority of India (UIDAI). The notification was issued for the purpose of implementing the Unique Identity (UID) scheme, under which a UID database was to be created, using the biometric and demographic details of the residents of India. There was no mention of collection of biometric information in the said notification, or of any provisions for commercialisation of the material. The notification also did not provide any checks and balance over the manner in which the information was to be collected, stored, or used under the UID scheme.
23. The petitioners herein challenged the entirety of the Aadhaar project in a Writ Petition (Civil) No. 829 of 2013 filed in this Hon'ble Court.
24. On 11.08.2015, a three-judge bench of this Hon'ble Court referred the question on the existence of a fundamental right to privacy to a

Constitutional bench. This was finally referred to a nine-judge bench in 2017.

25. In 2016, the Aadhaar Act was passed in the Lok Sabha. It was passed as a money bill under Article 110 of the Constitution, which bypassed the Rajya Sabha.
26. The petitioners herein filed Writ Petition (Civil) 797 of 2016, titled '*S.G. Vombatkere and Anr. vs. Union of India &Anr.*', challenging the Aadhaar Act.
27. In 2017, a nine-judge Constitution Bench of this Court issued the "Privacy Judgement," on the issue of the existence of the fundamental right to privacy in W.P. (Civil) 494 of 2012, titled "*Justice K.S. Puttaswamy (Retd.) &Anr. V. Union of India &Ors.*" and other matters. This Court unanimously held that there exists a fundamental right to privacy, and remitted the matter as relating to the constitutionality of the Aadhaar Act back for adjudication. The 'Privacy Judgment' is reported at (2017) 10 SCC 1.
28. On 26.08.2018, a five-judge bench of this Hon'ble Court rendered three separate judgments in the "Aadhaar Case," (*Justice Puttuswamy (Retd.) vs. Union of India &Anr.*). Dr. A.K. Sikri, J. (for himself as well as Dipak Mishra, CJI and A.M. Khanwilkar, J.) authored the majority judgment. Ashok Bhushan, J. rendered a separate judgment which broadly concurred with the majority judgment. These two judgments are together referred to as the 'Majority Judgments'. The third dissenting judgment of the Court was rendered by Dr. D.Y. Chandrachud, J. The Aadhaar Judgement is reported at (2019) 1 SCC 1.

The judgment significantly read down the Aadhaar project and directed that the use of Aadhaar be restricted for only **two** purposes, and only by the government. The two permitted purposes were: -

- For the purposes laid out under Section 7 of the Aadhaar Act, wherein Aadhaar linkage and verification could be made mandatory for the disbursal of government benefits, subsidies and services funded by the Consolidated Fund of India; and
- Under Section 139AA of the Income Tax Act, 1961, under which Aadhaar linkage was mandatory with respect to a PAN card.

29. The Aadhaar and Other Laws (Amendment) Bill, 2018 (**"Aadhaar Amendment Bill"**) was passed in Lok Sabha on 04.01.2019, after one day of debate. It was then pending before the Rajya Sabha, when the Lok Sabha dissolved.

30. The Aadhaar Amendment Bill lapsed.

31. The Aadhaar and Other Laws (Amendment) Ordinance, 2019 was promulgated by the President of India on 2<sup>nd</sup> March 2019. The impugned Ordinance is identical to the Aadhaar Amendment Bill, which lapsed.

32. On 7.03.2019, the UIDAI notified the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 under which UIDAI will charge private entities Rs.20 per e-KYC transaction, and Rs.0.50 per Yes/No authentication transaction.

F. LACK OF INTEGRITY IN AADHAAR DATABASE

33. The Petitioners state that the database of demographic and biometric information collected and stored by the 2<sup>nd</sup> Respondent lacks integrity.
34. The demographic data as well as the biometric data uploaded/captured at the time of enrolment and /or updation is carried out without any verification by a government official.
35. The data stored with the 2<sup>nd</sup> Respondent is based on a system of "self-certification" where an individual states that certain information relating to herself such as her name, date of birth, address, mobile number, email or residence status are indeed correct. This is done without verification on the part of any government official and without any check regarding the address submitted.
36. The 2<sup>nd</sup> Respondent is not in a position to and does not certify the accuracy of the demographic data as well as the biometric data with respect to an individual.
37. The 2<sup>nd</sup> Respondent takes no responsibility with respect to the correctness of the biometrics or the demographics or the residence status of the person who has enrolled.
38. In the backdrop of the undisputed facts set out in this section of the petition in the paragraphs immediately preceding, it is reckless on the part of the Respondents to allow e-KYC or identification based on the Aadhaar database. The Aadhaar database is a Trojan Horse which will overtime infect, undermine and debase the integrity of the databases of services covered by section 4 of the Indian Telegraph Act 1885 and Chapter IV of the Prevention of Money Laundering Act, 2002.

**G. THE SURVEILLANCE ARCHITECTURE**

39. The architecture and design of the Aadhaar project enables mass surveillance of persons enrolled under the Aadhaar Act. Under the Aadhaar project, enrollees are assigned an Aadhaar number against their biometrics and demographic details, which are stored in a centralized database ("CIDR"). A log of the movements through the Aadhaar system, in the form of biometric capture and authentication, is retained in the centralized database. This enables surveillance of residents either by someone within the system, or through unauthorized access to the system in the following manner:

- (i) Each and every electronic device that is linked to the internet has a unique identification. This is similar to a vehicle registration number or a cellular telephone number or a cheque number which makes that item uniquely identifiable.
- (ii) In addition to this generic "unique identification", when an electronic device is linked to the Aadhaar system /server /CIDR, the devices electronically exchange information and at this stage the Aadhaar system will designate a unique identification number to a particular device which is called its registered device ID. This registered device ID is designed to be the permanent ID in respect of that device qua Aadhaar. Illustratively, if a finger print is being read by a particular authentication device and this authentication device is linked to the Aadhaar System, Aadhaar will designate a specific ID to that device at the first interaction and thereafter whenever that device is linked to Aadhaar, the transmission will be recognized as emanating from that device.

(iii) The transmission between the external device (now with its registered device ID) and the Aadhaar server will be carried on a network comprising wire, as well as wireless systems. Regardless of whether the message is being transmitted through the medium of wire or wireless, a unique electronic path attaches to each transmission. This unique electronic path identifies the links through which the message is transmitted and each of these links is uniquely identifiable.

(iv) In other words, in a transmission between a registered device (e.g. finger print reader) and the CIDR it is technically possible to track and trace the electronic route taken by every transmission.

This implies that it is possible to electronically track down the location of every registered device in real time. This is because the Respondents themselves project that the authentication transaction comprising a cycle of request and response can be completed in as little as 3 to 5 seconds.

(v) Hypothetically, in a situation where Aadhaar authentication is required at the stage of say withdrawing money from an ATM, clocking in at a government office and receiving an LPG cylinder would mean that each of these stages the physical location as well as the nature of the transaction would be known to the Respondents or would be easily discernible by the Respondents.

40. This explanation/illustration is irrefutable and clearly brings out the nature of a surveillance state sanctioned by the Aadhaar Act and strengthened by the impugned Ordinance. The manner in which the Aadhaar CIDR is able to provide authentication and deliver its

confirmation/refusal to a particular device is because the electronic path and the terminal device is identifiable and can be easily traced back.

41. The extent and pervasiveness of the surveillance over time will deepen with the addition of players and entities, including private entities, that are entitled to utilize the Aadhaar ecosystem and the authentication facility. This is specifically sanctioned by Sections 5, 24 and 25 of the impugned Ordinance. The UIDAI will have little or no incentive to restrict the use of authentication through the Aadhaar system considering that the impugned Regulations permit the use of fingerprints as commerce.

42. The upshot is that if the impugned Ordinance is allowed to stand, the State will have a capacity to very easily track down and trace the physical location of every individual seeking authentication with reasonable accuracy and will also have the capacity to assess the nature of the activity the person is engaged in. It is respectfully submitted that the affidavits and reports of technically qualified persons appended to this petition (and also placed before the Supreme Court by the petitioners in the Aadhaar case) establish how the Aadhaar project increases the capacity of an authoritarian Police State. These experts are unanimous in concurring that the architecture and design of Aadhaar enable real time surveillance:

(i) Dr. Samir Kelekar in an affidavit dated 6.4.2016 filed on behalf of the petitioners in the Aadhaar case (and re-verified for this petition by an affidavit dated 2.04.2019) states:

*"That as someone with fairly extensive experience of cyber security, I can categorically state that this project is highly imprudent, as it throws open the clear possibility of*

*compromising basic privacy by 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 said authority or authentication data traffic as the case may be.*

*That I state that I have perused the documents that UIDAI have put out in relation to the design of the Aadhaar authentication system, and I can categorically state it is quite easy to know the place and type of transaction every time such authentication takes place using a scanner for fingerprints or iris and the records of these in the UID / "Aadhaar" database. Knowing the various types of transactions done via a particular Aadhaar number would help UIDAI or related parties to track the behaviour of a person using Aadhaar.*

*Further, I also point out that UIDAI recommends that each point of service device i.e. the device from which an authentication request emanates, register itself with the UIDAI and acquire for itself a unique device ID, which shall then be passed to UIDAI along with the request for every authentication transaction. I state herein that the said method of uniquely identifying every device and being able to map every authentication transaction to be emanating from a unique registered device, further makes the task of tracking down the place from which an authentication request emanates easier."*

Dr. Samir Kelekar's affidavit dated 02.04.2019 along with a copy of his affidavit dated 6.4.2016 is filed herewith as **ANNEXURE P-5 at pages 79 to 84.**

- (ii) Jude Terrence D'Souza in an affidavit dated 22.11.2016 filed on behalf of the petitioners in the Aadhaar case (and re-verified for this petition by an affidavit dated 11.04.2019) states:

*"At the time of each and every request for authentication / verification, the finger print reader is required to electronically indicate its unique identification number to the central depository server. Combining the unique number of the finger print reader with the in-built GPS, the location of the individual whose finger print is being verified becomes known, virtually in real time. The verification system is so designed that it can operate as a real time surveillance system of every individual who is required to give his / her finger print for the purpose of authentication.*

***As the Aadhaar verification system is used progressively in more and more applications, the extent and pervasiveness of the surveillance will increase.***

*By way of illustration, if Aadhaar verification using a fingerprint reader is carried out at say an airport for boarding an aircraft or at a public distribution shop for collection rations or for withdrawing money from an Automatic Teller at a bank (ATM), the State will know the precise location of the individual.*

*Even if the GPS systems is disabled, since the fingerprint reader is communicating with the central depository through an electronic connection, it is easily possible to locate the finger print reader and in that manner, the place where the individual seeking verification is located."*

(emphasis supplied)

Jude Terrence D'Souza's affidavit dated 11.04.2019 along with a copy of his affidavit dated 22.11.2016 is filed herewith as

**ANNEXURE P-6 at pages 85 to 95.**

43. The petitioner's concerns regarding a surveillance State and a surveillance society under the Aadhaar project are corroborated by a report of Dr. Manindra Agrawal, N. Rama Rao Professor at IIT Kanpur

dated 04.03.2018, filed by way of IA No. 34627/2018 in WP (C) No. 494 of 2012 on behalf of the Respondents during the hearing of the Aadhaar case. This report states:

*"Finally let us turn attention to Verification Log. Its leakage may affect both the security and the privacy of an individual as one can extract identities of several people... and also locate the places of transactions [done] by an individual in the past five years... Tracking current location is possible."*

A copy of Dr. Manindra Agrawal's report dated 04.03.2018 is filed herewith as **ANNEXURE P-7 at pages 96 to 102**.

44. As Justice Chandrachud's judgment in the Aadhaar judgment correctly records, Prof. Manindra Agarwal's report indicates the possibility of the Aadhaar database being used to track the location of an individual. This finding by the only Learned Judge who considered the expert evidence illustrates the danger of allowing more entities to access the Aadhaar system, which the impugned Ordinance enables and the impugned Regulations incentivise.

**H.GROUNDS TO CHALLENGE THE AADHAAR AND OTHER LAWS (AMENDMENT) ORDINANCE, 2019 (NO. 9 OF 2019)**

45. The Petitioners submit that the Aadhaar and Other Laws (Amendment) Ordinance, 2019 (No. 9 of 2019) ("**impugned Ordinance**") is *ultra vires*, illegal, null and void on the following grounds, amongst others. These grounds are set out hereafter and are without prejudice to one another:

- A. The impugned Ordinance is unconstitutional as it violates the rights guaranteed under Part III of the Constitution. It enables State surveillance and private surveillance of citizens, and commercial

exploitation of personal information that is collected and stored for State purposes.

- **Private surveillance**

(a) It has been held by the majority judgment in the Aadhaar case:

*"513.8.3. Apart from authorising the State, even "anybody 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."*

(Emphasis supplied)

(b) The Aadhaar judgement upheld the constitutionality of the Aadhaar project by restricting the use of the project to limited circumstances, and that too, only by the State. Essential to this was a total restraint on private parties from accessing the Aadhaar system for commercial purposes.

(c) The majority judgment in the Aadhaar case found that the Aadhaar Act and project did not enable a surveillance state *after* striking down certain offending provisions including (i) Section 57 of the Aadhaar Act; (ii) Rule 9 of the Prevention of Money-laundering (Maintenance of Records) Seventh Amendment Rules,

2017; and (iii) a circular dated 23.3.2017 issued by the Department of Telecommunications. Even with respect to the use of the Aadhaar system by the State, the Supreme Court limited this to two circumstances:

(i) use under Section 7 of the Aadhaar Act strictly for the disbursement of subsidies, benefits and services funded by the Consolidated Fund of India; and

(ii) use under Section 139AA of the Income Tax Act, 1961.

(d) The impugned Ordinance goes against this unequivocal restriction by opening up the Aadhaar system to private entities. This is constitutionally impermissible.

Sections 5, 24 and 25 of the impugned Ordinance effectively restore the offending provisions that were struck down as unconstitutional by the Supreme Court. This finding of unconstitutionality on account of possibility of surveillance will extend to voluntary use and authentication, as presently contemplated under the impugned Ordinance.

(e) While striking down the circular dated 23.3.2017 issued by the Department of Telecommunications, the majority judgement in the Aadhaar case held that the circular failed to meet the proportionality test under Part III of the Constitution.

*"(442) We are of the opinion that not only such a circular lacks backing of a law, it fails to meet the requirement of proportionality as well. It does not meet 'necessity stage' and 'balancing stage' tests to check the primary menace which is in the mind of the respondent authorities. There can be other appropriate laws and less intrusive alternatives. For*

*the misuse of such SIM cards by a handful of persons, the entire population cannot be subjected to intrusion into their private lives."*

(emphasis supplied)

Justice Chandrachud, while concurring, noted:

*"...In applying the test of proportionality, the matter has to be addressed not just by determining whether a measure is efficient but whether it meets the test of not being disproportionate or excessive to the legitimate aim which the state seeks to pursue. TRAI and DoT do have a legitimate concern over the existence of SIM cards obtained against identities which are not genuine. **But the real issue is whether the linking of Aadhaar cards is the least intrusive method of obviating the problems associated with subscriber verification. The state cannot be oblivious to the need to protect privacy and of the dangers inherent in the utilization of the Aadhaar platform by telecom service providers. In the absence of adequate safeguards, the biometric data of mobile subscribers can be seriously compromised and exploited for commercial gain. While asserting the need for proper verification, the state cannot disregard the countervailing requirements of preserving the integrity of biometric data and the privacy of mobile phone subscribers. Nor can we accept the argument that cell phone data is so universal that one can become blasé about the dangers inherent in the revealing of biometric information."***

(emphasis supplied)

- The consequence of expanding the use of Aadhaar to private entities is the creation of federated databases which compromises peoples' fundamental right to privacy. This is

validated by recent news reports regarding the misuse of Aadhaar data. In February 2019, it was reported that "Sevamitra," a privately developed application created by the incumbent Telugu Desam Party, misused the demographic data of 3.7 crore voters in Andhra Pradesh. This application used data collated for a State survey (Smart Pulse Survey) relying on the demographic information collected for Aadhaar cards, electoral rolls and socio-economic data collected by the State welfare departments.

- Newspaper articles entitled (i) "IT firm working on app for TDP 'stole' data of Andhra voters, say cops," Sreenivas Janyala, INDIAN EXPRESS dated 05.03.2019; are annexed as **ANNEXURE P-8 pages 103 to 105.**
- Newspaper articles entitled (ii) "TDP app breached data of 3.7cr voters? Probe begins," Times News Network dated 26.02.2019 **P-9 at pages 106 to 108**.
- FIR dated 02.03.2009 filed by one, Thumalla Lokeswara Reddy under Sections 66-B and 72 of the Information Technology Act, 2000 and Sections 120b, 379, 420 and 188 of the Indian Penal Code regarding the misuse of demographic data, including Aadhaar data, by the abovementioned TDP app is annexed herewith as **ANNEXURE P-10 at pages 109 to 112.**

(f) In the Privacy Judgement, the fundamental right to privacy has also been recognised as a horizontal right against non-State actors. Every private entity which has access to the Aadhaar

database is therefore under a public duty to ensure that the information accessible to it through the Aadhaar database, including Aadhaar numbers, is not: (i) stored by the private entity for further commercial or other use; (ii) seeded with any other database; or (iii) used for commercial profiling.

- **Surveillance architecture**

(g) By permitting private entities to join the Aadhaar ecosystem, the impugned Ordinance exacerbates the threat of surveillance that the Aadhaar project poses. The architecture and design of the Aadhaar project enable mass surveillance. Increasing the number of entities which are allowed access to the Aadhaar database increases this risk of surveillance exponentially.

(h) The centralized database (CIDR) is controlled and managed by the UIDAI, which is State under Article 12 of the Constitution of India. The Constitution of India does not permit a system that allows mass surveillance, tracking and profiling of individuals, or the exacerbation of this threat through increasing the number of entities that can join this ecosystem. The Supreme Court ought to prevent the advent of a surveillance society, even where individual citizens may 'volunteer' to be electronically tethered to a State-operated computer system that can trace their location in real time.

(i) The Supreme Court in *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others* (9-Judges) has recognised that mass surveillance measures adopted by the State invade the right to privacy.

Justice Chandrachud in the majority decision, *inter alia*, held:

*"51...The observations in Malak Singh on the issue of privacy indicate that an encroachment on privacy infringes personal liberty under Article 21 and the right to the freedom of movement under Article 19(1)(d). Without specifically holding that privacy is a protected constitutional value under Article 19 or Article 21, the judgment of this Court indicates that serious encroachments on privacy impinge upon personal liberty and the freedom of movement. The Court linked such an encroachment with the **dignity of the individual which would be offended by surveillance bereft of procedural protections and carried out in a manner that would obstruct the free exercise of freedoms guaranteed by the fundamental rights.**"*

134 (ii)... The development of the jurisprudence on the right to privacy in the United States of America shows that even though there is no explicit mention of the word 'privacy' in the Constitution, the courts of the country have not only recognised the right to privacy under various Amendments of the Constitution but also progressively extended the ambit of protection under the right to privacy. In its early years, the focus was on property and protection of physical spaces that would be considered private such as an individual's home. This 'trespass doctrine' became irrelevant when it was held that what is protected under the right to privacy is "people, not places". The 'reasonable expectation of privacy' test has been relied on subsequently by various other jurisdictions while developing the right to privacy. Having located the right to privacy in the 'person', **American jurisprudence on the right to privacy has developed to shield various private aspects of a person's life from interference by the state - such as conscience, education,**

*personal information, communications and conversations, sexuality, marriage, procreation, contraception, individual beliefs, thoughts and emotions, political and other social groups. Various judgments of the Court have also analysed technological developments which have made surveillance more pervasive and affecting citizens' privacy. In all these cases, the Court has tried to balance the interests of the individual in maintaining the right to privacy with the interest of the State in maintaining law and order."*

(emphasis supplied)

Justice Kaul in his concurring opinion, *inter alia*, held:

*"13. The growth and development of technology has created new instruments for the possible invasion of privacy by the State, including through surveillance, profiling and data collection and processing. Surveillance is not new, but technology has permitted surveillance in ways that are unimaginable. Edward Snowden shocked the world with his disclosures about global surveillance. States are utilizing technology in the most imaginative ways particularly in view of increasing global terrorist attacks and heightened public safety concerns. One such technique being adopted by States is 'profiling'."*

(emphasis supplied)

- (i) Justice Chandrachud in the Aadhaar judgement has specifically held that the Aadhaar architecture has created an opportunity for surveillance and large-scale profiling:

*"1152. Technology today brings with it tremendous power and is much like two sides of a coin. When applied productively, it allows individuals around the world to*

*access information, express themselves and participate in local and global discussions in real-time in ways previously thought unimaginable. The flip side is the concern over the abuse of new technology, including biometrics, by the State and private entities by actions such as surveillance and large-scale profiling. This is particularly acute, given the fact that technological advancements have far outpaced legislative change. As a consequence, the safeguards necessary to ensure protection of human rights and data protection are often missing. The lack of regulatory frameworks, or the inadequacy of existing frameworks, has societal and ethical consequences and poses a constant risk that the concepts of privacy, liberty and other fundamental freedoms will be misunderstood, eroded or devalued...*

*1156. The collection of most forms of biometric data requires some infringement of the data subject's personal space. Iris and fingerprint scanners require close proximity of biometric sensors to body parts such as eyes, hands and fingertips. Even in the context of law enforcement and forensic identification, the use of fingerprinting is acknowledged to jeopardise physical privacy. Many countries have laws and regulations which are intended to regulate such measures, in order to protect the individual's rights against infringement by State powers and law enforcement. However, biometrics for the purpose of authentication and identification is different as they do not have a specific goal of finding traces related to a crime but are instead conducted for the purpose of generating identity information specific to an individual. This difference in purpose actually renders the collection of physical biometrics a more serious breach of integrity and privacy. It indicates that there may be a presumption that someone is guilty until proven innocent. This would be*

*contrary to generally accepted legal doctrine that a person is innocent until proven guilty and will bring a lot of innocent people into surveillance schemes.*

*1539. The violations of fundamental rights resulting from the Aadhaar Scheme were tested on the touchstone of proportionality. The measures adopted by the respondents fail to satisfy the test of necessity and proportionality for the following reasons:*

*1539.1. Under the Aadhaar Project, Requesting Entities can hold the identity information of individuals, for a temporary period. It was admitted by Uidai that AUAs may store additional information according to their requirement to secure their system. ASAs have also been permitted to store logs of authentication transactions for a specific time period. It has been admitted by Uidai that it gets the AUA code, ASA code, unique device code and the registered device code used for authentication, and that Uidai would know from which device the authentication took place and through which AUA/ASA. Under the Regulations, Uidai further stores the authentication transaction data. This is in violation of widely recognised data minimisation principles which mandate that data collectors and processors delete personal data records when the purpose for which it has been collected is fulfilled. Moreover, using the metadata related to the transaction, the location of the authentication can easily be traced using the IP address, which impacts upon the privacy of the individual.*

*1539.2. From the verification log, it is possible to locate the places of transactions by an individual in the past five years. It is also possible through the Aadhaar database to track the current location of an individual, even without the verification log. The architecture of Aadhaar poses a risk of potential surveillance activities through the Aadhaar*

*database. Any leakage in the verification log poses an additional risk of an individual's biometric data being vulnerable to unauthorised exploitation by third parties.*

*1539.3. The biometric database in the CIDR is accessible to third-party vendors providing biometric search and de-duplication algorithms, since neither the Central Government nor Uidai have the source code for the de-duplication technology which is at the heart of the programme. The source code belongs to a foreign corporation. Uidai is merely a licensee. Prior to the enactment of the Aadhaar Act, without the consent of individual citizens, Uidai contracted with L-1 Identity Solutions (the foreign entity which provided the source code for biometric storage) to provide to it any personal information related to any resident of India. This is contrary to the basic requirement that an individual has the right to protect herself by maintaining control over personal information. The protection of the data of 1.2 billion citizens is a question of national security and cannot be subjected to the mere terms and conditions of a normal contract.*

*1539.9. Allowing private entities to use Aadhaar numbers, under Section 57, will lead to commercial exploitation of the personal data of individuals without consent and could also lead to individual profiling. Profiling could be used to predict the emergence of future choices and preferences of individuals. These preferences could also be used to influence the decision-making of the electorate in choosing candidates for electoral offices. This is contrary to privacy protection norms. Data cannot be used for any purpose other than those that have been approved. While developing an identification system of the magnitude of Aadhaar, security concerns relating to the data of 1.2 billion citizens ought to be addressed. These issues have*

*not been dealt with by the Aadhaar Act. By failing to protect the constitutional rights of citizens, Section 57 violates Articles 14 and 21.*

*1539.10. Section 57 is susceptible to be applied to permit commercial exploitation of the data of individuals or to affect their behavioural patterns. Section 57 cannot pass constitutional muster. Since it is manifestly arbitrary, it suffers from overbreadth and violates Article 14.*

*1539.13. When Aadhaar is seeded into every database, it becomes a bridge across discreet data silos, which allows anyone with access to this information to reconstruct a profile of an individual's life. This is contrary to the right to privacy and poses severe threats due to potential surveillance."*

(k) The architecture of surveillance under the Aadhaar Act and project has been confirmed by three experts who had filed affidavits / reports before the Supreme Court in the Aadhaar case.

All three experts were unanimous in concurring that the design of Aadhaar enabled real time surveillance.

B. The Aadhaar database lacks integrity and has no value other than, at most, the underlying documents on the basis of which the Aadhaar numbers are issued. The use of Aadhaar for the purposes of Know Your Customer ("KYC") requirements (including e-KYC) and the verification of identity through Aadhaar threatens to compromise the efficacy of the extant KYC procedures and weaken the existing safeguards for the prevention of money laundering. The Aadhaar

database is nothing but a Trojan Horse that will bring unverified people into existing databases.

(a) As per the admissions of the UIDAI in the Aadhaar case, data submitted for the generation of an Aadhaar number is self-certified by the person being enrolled and is not verified by the UIDAI. The authority takes no responsibility for the correctness of the details submitted to it, the genuineness of the documents submitted, or even whether the person enrolling is an illegal immigrant. This form of identification for bank accounts and mobile connections is a threat to national security and the financial integrity of the country.

(b) The inevitable consequence is that the UIDAI is sitting on a heap of data lacking in integrity and fidelity. An identification programme built on such data is palpably arbitrary and of no value. Justice Chandrachud in the Aadhaar judgment notes:

*"1332...the correctness of the documents submitted by an individual at the stage of enrolment or while updating information is not verified by any official of UIDAI or of the Government."*

(c) In the Aadhaar case, the UIDAI admitted:

- No UIDAI or Government official verifies the correctness of documents offered at the stage of enrolment / updating;
- UIDAI takes no responsibility with respect to the correctness of the biometrics, name, date of birth,

address, mobile number, email id or resident status of the person enrolled;

- UIDAI does not know whether the documents shown at the time of enrolment / updating are genuine or false;
- At the stage of enrolment, there is no verification as to whether a person is an illegal immigrant;
- At the stage of enrolment, there is no verification about a person being resident in India for 182 days or more in the past 12 months (only self-declaration).
- UIDAI has no way of finding out a fake Aadhaar number, till such time a biometric mismatch takes place at the time of attempted authentication.

(d) Aadhaar is not a form of identity but a mode of identification. On being enrolled, a person is assigned a number. This number is allotted after a much lower level of scrutiny as compared to other Officially Valid Documents ("OVDs"). Each of the other OVDs are issued after government verification of the documents and information submitted by the enrolee. Including Aadhaar in the same bracket as the other OVDs for the purpose of verification of identity will dilute the legitimacy of the verification process. Section 24 and 25 of the impugned Ordinance which seeks to amend the Indian Telegraph Act, 1885 and Prevention of Money Laundering Act, 2002 respectively, suffer from over-inclusiveness and is unconstitutional.

(e) The Reserve Bank of India ('RBI') by way of circulars dated 27.01.2011 and 28.09.2011 had raised concerns relating to the exclusive reliance on Aadhaar for opening bank accounts. Copies of the relevant RBI circulars dated 27.01.2011 and 28.09.2011 are annexed hereto and marked as **ANNEXURE P-11 at pages 113 to 116 and P-12 at pages 117 to 119.**

(f) Furthermore, the efficacy of Aadhaar is dependent on other Proof of Identity and Proof of Address documents and not on independent verification of identity. This is outlined in the UIDAI's Demographic Data Standards and Verification Procedure ("**DDSV**") Report at 3.1, and Aadhaar Enrolment Form.

(g) The lack of value of the data in the Aadhaar database has been taken judicial notice of in recent judgments of two High Courts, which were given subsequent to the Aadhaar judgment.

- In an order dated 03.01.2019 in *Debashis Nandy v. Union of India*, a Single Judge of the Calcutta High Court noted that there was no verification of the authenticity of the demographic data in the Aadhaar database.

*"There is definitely something amiss with the Aadhaar enrolment process if important demographic information such as the name of the applicant's father, as in the case in hand, can be falsified and even go undetected."*

- In an order dated 09.01.2019 *Smt. Parvati Kumar v. State of U.P.*, a Division Bench of the Lucknow Bench of

the Allahabad High Court held:

*"We clearly deduce from the above that the other information namely name, date of birth, gender and address as entered in the Aadhaar Card, is furnished by the Aadhaar applicant at the time of authentication/enrolment. Although, the regulations provide for the applicant to rely on a set of documents for giving information in regard to name, address and proof of date of birth, however, because the said information is merely given by the applicant, and is not authenticated by UIDAI at the time of authentication, the Aadhaar Card cannot be conclusive proof in regard to those entries."*

(h) There is no independent government or UIDAI verification of the data collected for Aadhaar enrolment and the process of building the Aadhaar database permits large scale fraud. There have been several reported instances of generation of fake Aadhaar numbers.

In January 2019, the State Bank of India informed UIDAI that there had been large-scale fraudulent Aadhaar enrolments through its enrolment centres in November 2018. State Bank of India officials indicated that the log-in details and biometrics of their operators had been used to generate fake and unauthorised Aadhaar numbers.

Newspaper reports entitled (i) "SBI alleges Aadhaar data misuse, UIDAI rubbishes charge," published in the TIMES OF INDIA dated 29.01.2019; and (ii) "Aadhaar details of enrolment operator stolen and misused, show UIDAI records: Report," published in SCROLL dated 20.02.2019, are annexed herewith as **ANNEXURE P-13** at

pages 120 to 124 and ANNEXURE P-14 at pages 125 to 126.

(i) In view of the lack of sanctity of the Aadhaar database, Sections 24 and 25 of the impugned Ordinance, which amend the Prevention of Money Laundering Act, 2002 and the Indian Telegraph Act, 1885 and permit the use of Aadhaar numbers for verification of identity, are manifestly arbitrary and violate Article 14 of the Constitution of India. There are numerous, more reliable, certified, less invasive and less disruptive methods of verifying the identity of citizens. In view of Articles 14 and 21 of the Constitution of India, the impugned Ordinance permits invasion of the right to privacy, is grossly disproportionate, manifestly arbitrary and should be struck down.

(j) The Supreme Court in the Aadhaar judgment acknowledged the existence of illegal immigrants and non-residents in the Aadhaar database. A specific direction was given by the Supreme Court to the UIDAI,

*"394. Insofar as Section 2(v) is concerned which defines resident, there is nothing wrong with the definition. The grievance of the petitioners is that the Aadhaar Act creates no credible machinery for availing a claim that a person has been residing in India for 182 days or more. Apprehension is expressed that this expression may also facilitate the entry of illegal immigrants. These aspects can be taken care of by the respondents by providing appropriate mechanism. We direct the respondents to do the needful in this behalf.*

*However, that would not render the definition unconstitutional."*

However, till date the UIDAI has not taken any tangible steps to ensure compliance of the aforesaid direction. Absent such steps taken to cleanse the Aadhaar database, the use of the database for the purpose of e-KYC is manifestly arbitrary. The impugned Ordinance which facilitates the same is unconstitutional for this ground alone.

C. Section 7 read with Section 2(v) of the impugned Ordinance which introduces Section 8A to the Aadhaar Act, creates a new mode of verification through the Aadhaar system called "offline verification". This is a mode of verification of identity without authentication, using offline systems. Offline verification is undertaken through the use of Quick Response codes ("QR codes") printed on Aadhaar "cards," e-Aadhaars or a downloaded XML file. The QR codes store demographic information and a photograph of the Aadhaar number holder as available in the CIDR, along with an electronic signature of the UIDAI. To enable offline verification, the UIDAI digitally signs the information stored in the QR codes. When a request for offline verification is made, the service provider scans the QR Code, verifies the digital signature and accesses the data encrypted in this code. Permitting verification of identity in this manner is manifestly arbitrary for the following reasons:

(a) UIDAI's claims regarding enhanced accuracy of verification of identity through the Aadhaar system was based on the purported

infallibility of biometric de-duplication and online authentication through real-time communication with the CIDR. Offline verification eliminates real-time communication with the CIDR and further diminishes the value that can be attached to verification of identity through a database built on self-certified information.

(b) UIDAI is no longer involved in the verification of identity through authentication. This makes identity theft even easier. Whoever has access to the QR code of another person also has continuous access to her demographic information and photograph. UIDAI has no manner of determining if the verification is being requested by the person enrolled on its database or by an impersonator. The impugned Ordinance introduces no additional provisions to prevent, discover or punish such abuse of the Aadhaar database and leaves the citizens completely exposed to an increased risk of identity theft.

(c) Opportunities to save Aadhaar numbers and the related data and information in offline federated databases are reinforced and strengthened under the system of offline verification. This is not only impermissible under the Aadhaar Act, but also unconstitutional inasmuch as it enables private entities to store and commercialise citizen's personal data. It also exacerbates the possibility of profiling.

(d) Section 8A of the Aadhaar Act, as introduced by the impugned Ordinance, sets out certain conditions under which offline verification may be carried out. The provision states that offline verification can be undertaken only with informed consent and for

a limited, specified purpose. However, there is no guidance regarding the form of offline verification apart from excluding authentication. The only – and limited – sanctity of the Aadhaar number so far was in triggering authentication against the CIDR database through biometric de-duplication. The foreseeable impact of a provision that proposes to bypass this is a surfeit of bogus or fake Aadhaar “cards”. Offline verification therefore poses a grave threat to national security and the financial integrity of the country.

D. Reliance on Aadhaar in any form for meeting KYC obligations or for verifying identity constitutes a serious compromise of India’s commitments under international law and policy, as enlisted below. Under these, banks were advised to follow certain customer identification procedures for opening of accounts and monitoring transactions of a suspicious nature for the purposes of reporting it to appropriate authority. These ‘Know Your Customer’ guidelines have been made a part of domestic law through legislation such as the Prevention of Money Laundering Act, 2002 and periodic circulars and guidelines issued by the RBI. The impugned Ordinance compromises India’s international law obligations which are required to be respected under Article 51 of the Constitution of India. These commitments arise under the following:

- a. Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT),

- b. the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision,
  - c. United Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,
  - d. Political Declaration and Global Programme of Action, annexed to the resolution S-17/2 was adopted by the General Assembly of the United Nations in February 1990,
  - e. Political Declaration adopted in Special Session of the United Nations General Assembly in June 1998.
- E. The impugned Ordinance refers to free and informed consent. This consent and the proposed scheme of "voluntariness" in the use of Aadhaar is however illusory in view of Section 4(7) of the Aadhaar Act, introduced by the impugned Ordinance.
- (a) Under Section 4(7) of the Aadhaar Act, the Parliament can make Aadhaar authentication mandatory for any purpose. The impugned Ordinance does not prescribe any standards or guidance for such mandatory use of Aadhaar authentication. An Aadhaar holder therefore cannot envisage the myriad uses to which the Aadhaar data can be put now and in the future.
  - (b) The notion of "informed consent," was already present in the earlier iteration of the Aadhaar Act. Section 8(2)(a) of the Aadhaar Act required requesting entities to obtain the consent of persons whose details were being used for authentication, and Section 8(3) mandated that this consent should be "informed consent" by requiring that an individual submitting her identity

information for authentication shall be informed of the nature and the use of the information that may be shared upon authentication and the alternatives to submission of identity information to the requesting entity. Despite these provisions, the Supreme Court emphasised the need for strictly voluntary use of Aadhaar, which Section 4(7) introduced by the impugned Ordinance seeks to eliminate.

(c) Including the concepts of voluntariness and consent cannot make a project that is unconstitutional on account of violation of Part III rights, constitutional. There can be no waiver of fundamental rights and the State cannot put its citizens in a situation where they are constrained to "voluntarily" offer up these rights in exchange for an ostensibly efficient or convenient system.

(d) The national motto is "let truth prevail." No statutory form can compel citizens to make false declarations. In the circumstances, the expression "free and voluntary," appearing at the head of the form is liable to be removed. In the alternative, citizens who are being forced to enrol, may be permitted to paste a written declaration that they are enrolling under protest.

F. The impugned Ordinance amends Section 33(2) of the Aadhaar Act and now permits disclosure of information on the grounds of national security, on the order of an officer who is not less than the rank of Secretary. This provision is contrary to the Aadhaar judgement which holds that the power of releasing sensitive information cannot be wielded without judicial review.

"409. Having regard to the aforesaid legal position, disclosure of information in the interest of national security cannot be faulted with. However, we are of the opinion that giving of such important power in the hands of Joint Secretary may not be appropriate. There has to be a higher ranking officer along with, preferably, a Judicial Officer. The provisions contained in Section 33(2) of the Act to the extent it gives power to Joint Secretary is, therefore, struck down giving liberty to the respondents to suitably enact a provision on the aforesaid lines, which would adequately protect the interest of individuals."

G. The Executive's power to promulgate ordinances under Article 123 of the Constitution of India was improperly exercised to amend the Aadhaar Act, the Indian Telegraph Act, 1885, and the Prevention of Money Laundering Act, 2002.

(a) Under Article 123, the ordinance making power is intended to meet extraordinary situations and should not be perverted to serve political ends. In *Krishna Kumar v. Union of India* ((2017) 3 SCC 1) a 7-judge bench of the Supreme Court held:

"41...Legislation by Ordinance is not an ordinary source of power making but is intended to meet extraordinary situations of an emergent nature, during the recess of the legislature..."

The 7-Judge bench also reaffirmed the principle laid down by the Supreme Court in *A.K. Roy v. Union of India* ((1982) 1 SCC 271):

"16...The Constituent Assembly held forth, as it were an assurance to the people that an extraordinary power shall not be used in order to perpetuate a fraud on the Constitution which is conceived with so much faith and vision..."

(b) The Aadhaar Amendment Bill was passed by the Lok Sabha after a cursory debate and was pending consideration before the Rajya Sabha before the dissolution of the concerned Parliamentary session. Without indicating any "extraordinary situation of an emergent nature", the Executive issued the impugned Ordinance, which is identical to the Aadhaar Amendment Bill. The impugned Ordinance has been issued absent a legal framework for data security in the country, to amend the Aadhaar Act, Indian Telegraph Act, 1885, and the Prevention of Money Laundering Act, 2002 merely to enable private entities to use the Aadhaar database.

H. The Aadhaar Act was passed as a Money bill. This was upheld on the ground that the Act was significantly related to the Consolidated Fund of India. Section 7 was read as the core provision of the Aadhaar Act, and the Supreme Court held that this provision has a substantial nexus with the Consolidated Fund of India. Further, the UIDAI is empowered to carry out various functions to facilitate its key role under Section 7, and this is funded by the Consolidated Fund of India. Section 10 of the impugned Ordinance amends Section 25 of the Aadhaar Act and funds received and earned by the UIDAI are now credited into a new Fund (the Unique Identification Authority of India Fund) instead of the Consolidated Fund of India. This severs the connection between the UID project and the Consolidated Fund of India. The UIDAI now has full autonomy to utilise the funds earned by it through commercialisation of the citizen's most intimate and personal data.

**I.GROUNDS TO CHALLENGE THE AADHAAR (PRICING OF AADHAAR AUTHENTICATION SERVICES) REGULATIONS, 2019**

46. The Petitioners submit that the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 (“**impugned Regulations**”) is *ultra vires*, illegal, null and void on the following grounds, amongst others. These grounds are set out hereafter and are without prejudice to one another:

A. The impugned Regulations which were notified in March 2019 direct private entities to pay for the e-KYC and authentication services provided by the UIDAI. Through these regulations, the UIDAI expressly seeks to commercialise, and gain financially through, large-scale collection of the citizen’s private data and the use of Aadhaar database by private entities. This is impermissible under our Constitutional scheme.

B. Peoples’ data, which was collected for the Aadhaar database, is their private property and permitting this to be commercialised is an impermissible violation of their dignity under Article 19 and 21 of the Constitution of India. Commercialising data relating to peoples’ bodies and lives is also a manifestly arbitrary measure. Further, it is contrary to the Privacy judgment which holds that people should have the right to control the commercial use of their data.

C. The impugned regulations permit fingerprints to be used as commerce. This is repugnant to the Constitutional protections accorded to our intimate details.

- D. The impugned Regulations incentivise UIDAI to multiply private entities using the Aadhaar database.
- E. Furthermore, in terms of Regulation 2(3) of the impugned Regulations incentivises the banks to enrol more individuals to meet the enrolments targets fixed by UIDAI. This results in lowering of checks and balances at the time of enrolment, as banks would find it more profitable to enrol an individual rather than reject it.

#### **J. JURISDICTION**

47. The present writ petition, under Article 32 of the Constitution of India, is being filed in public interest, to raise issues which endanger Fundamental Rights of citizens of India, protected under Articles 14, 19 and 21 of the Constitution. Having regard to the nationwide implications of the important issues raised in this petition, this Hon'ble Court ought to entertain and hear the present petition. The Petitioners states that they have not filed any other similar petition challenging the impugned Ordinance before this Hon'ble Court or any High Court. However, as set out above, the Petitioners have challenged the Aadhaar project in their previous writ petition (before enactment of the new law impugned herein).

#### **K. PRAYERS**

48. This Hon'ble Court may be pleased to issue appropriate declarations, writs, orders and directions as set out below:
- a) This Hon'ble Court may be pleased to issue an appropriate writ, order or direction in the nature of a mandamus to declare the

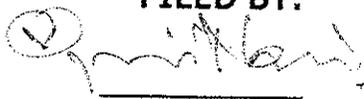
Aadhaar and Other Laws (Amendment) Ordinance, 2019 as ultra vires, unconstitutional, null and void and in particular violative of Articles 14, 19 and 21 of the Constitution of India.

- b) This Hon'ble Court may be pleased to issue an appropriate writ, order or direction in the nature of a mandamus to declare the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 as ultra vires, unconstitutional, null and void, and in particular violative of Articles 14, 19 and 21 of the Constitution of India.
- c) In the alternative, this Hon'ble Court may be pleased to issue an appropriate writ, order or direction in the nature of a mandamus to declare the following provisions of impugned Ordinance ultra vires and unconstitutional:
- (i) Section 5 of the impugned Ordinance which introduces Section 4(7) to the Aadhaar Act.
  - (ii) Section 7 of the impugned Ordinance which introduces Section 2(pa), 2(pb) and Section 8A to the Aadhaar Act and creates "offline verification".
  - (iii) Section 10 of the impugned Ordinance which creates the Unique Identification Authority of India Fund under Section 25 of the Aadhaar Act.
  - (iv) Section 12 of the impugned Ordinance, which amends Section 33(2) of the Aadhaar Act.
  - (v) Sections 24 and 25 of the impugned Ordinance, which amend the Prevention of Money Laundering Act, 2002 and the Indian Telegraph Act, 1885.

- d) This Hon'ble Court may be pleased to an appropriate writ, order or direction in the nature of a mandamus to declare that private entities which have access to the Aadhaar database are under a public duty to ensure that Aadhaar numbers and the data available through the Aadhaar database are not stored by these private entities.
- e) This Hon'ble Court may be pleased to an appropriate writ, order or direction in the nature of a mandamus to certify that no illegal immigrants have been issued Aadhaar numbers and that Aadhaar number which were issued to illegal immigrants have been omitted/deactivated.
- f) This Hon'ble Court may be pleased to award costs relating to the present petition to the Petitioners; and
- g) This Hon'ble Court may be pleased to issue any other writ/order/direction in the nature of mandamus as this Hon'ble Court may deem fit and proper in the circumstances of the case

AND FOR THIS ACT OF KINDNESS, THE PETITIONERS SHALL, AS IN DUTY BOUND, EVER PRAY

**DRAWN BY:**  
PRASANNA S.  
ADVOCATE

**FILED BY:**  
  
**VIPIN NAIR**  
ADVOCATE-ON-RECORD  
FOR THE PETITIONERS

DRAWN ON:-04.04.2019  
FILED ON:- 16.04.2019  
NEW DELHI

45 A

NOTARY REGISTER  
Sl. No. 60 Vol. No. 1  
Page No. 12 Dated 30-4-2019

IN THE SUPREME COURT OF INDIA  
CIVIL ORIGINAL JURISDICTION  
WRIT PETITION (C) NO. OF 2019

IN THE MATTER OF:

S.G. Vombatkere & Anr.

...Petitioners

Versus

Union of India & Ors.

...Respondent

AFFIDAVIT

I, SG Vombatkere, s/o Late V G Row, aged about 77 yrs, r/o 475, 7th Main Road, Vijayanagar, Mysore, Karnataka - 570017, do hereby solemnly affirm and state as under:

1. I am the Petitioner No.1 herein, I am fully conversant with the facts and circumstances of the Present case and am as such competent to swear the present affidavit on behalf of the Petitioners.
2. I say that I have no personal interest, motive, gain or oblique reasons in the filing of the accompanying Petition and the same is being filed purely in general public interest.

*S. G. Vombatkere*  
DEPONENT

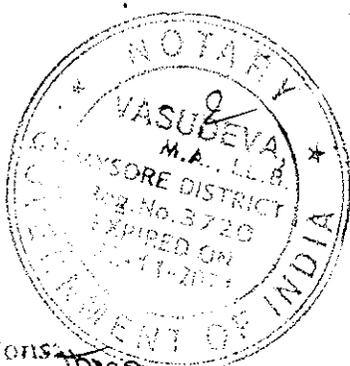
VERIFICATION:

Verified at MYSORU on this the 30th day of April 2019  
that the contents of paragraphs 1 to 2 of my above affidavit are true and correct to my knowledge, information and belief, that no part of it is false and nothing material has been concealed there from

*S. G. Vombatkere*

Solemnly Affirmed & Declared DEPONENT  
Before me on 30.04.2019

*U. Srinivas*  
NOTARY, MYSORE



46

IN THE SUPREME COURT OF INDIA  
CIVIL ORIGINAL JURISDICTION  
WRIT PETITION (C) NO. OF 2019

IN THE MATTER OF:

S.G. Vombatkere & Anr.

...Petitioners

Versus

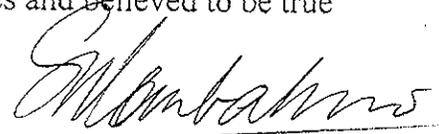
Union of India & Ors.

...Respondents

AFFIDAVIT

I, SG Vombatkere, s/o Late V G Row, aged about 77 yrs, r/o 475, 7th Main Road, Vijayanagar, Mysore, Karnataka - 570017, do hereby solemnly affirm and state as under:

1. I am the Petitioner No.1 herein, I am fully conversant with the facts and circumstances of the Present case and am as such competent to swear the present affidavit on behalf of the Petitioners.
2. I have read and understood the contents of the accompanying writ petition from pages 1 to 49 through - ; annexures thereto namely through - ; the Synopsis and the List of Dates from pages B to P through - and say that the facts set out therein are true to my knowledge and submissions made therein are on legal advice received from my Advocates and believed to be true and correct.

  
DEPONENT



No. of Corrections: *None*

47

**VERIFICATION:**

Verified at Mysore on this 24 day of April, 2019 that the contents of paragraphs 1 to 2 of my above affidavit are true and correct to my knowledge, information and belief, that no part of it is false and nothing material has been concealed there from.

*S. M. S. S.*

DEPONENT



Solemnly Affirmed & Declared  
Before me on 18 APR 2019

*[Signature]*  
NOTARY, MYSORE

No. of Corrections: None

47A

IN THE SUPREME COURT OF INDIA  
CIVIL ORIGINAL JURISDICTION  
WRIT PETITION (C) NO. OF 2019

IN THE MATTER OF:

S.G. Vombatkere & Anr.

...Petitioners

Versus

Union of India & Ors.

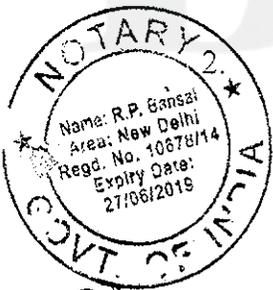
...Respondent

AFFIDAVIT

I, Bezwada Wilson, S/o Late Shri Yacob, aged about 48 years, R/o 36/13 Ground Floor, East Patel Nagar, New Delhi, do hereby solemnly affirm and state as under:

1. I am the Petitioner No.2 herein, I am fully conversant with the facts and circumstances of the Present case and am as such competent to swear the present affidavit on behalf of the Petitioners.

I say that I have no personal interest, motive, gain or oblique reasons in the filing of the accompanying Petition and the same is being filed purely in general public interest.



IDENTIFIED BY

DEPONENT

VERIFICATION:

Verified at Delhi on this the 2nd day of May 2019 that the contents of paragraphs 1 to 2 of my above affidavit are true and correct to my knowledge, information and belief, that no part of it is false and nothing material has been concealed there from.



ATTESTED  
Notary Public, Delhi  
(As Presented)

DEPONENT

48

IN THE SUPREME COURT OF INDIA  
CIVIL ORIGINAL JURISDICTION  
WRIT PETITION (C) NO. OF 2019

IN THE MATTER OF:

S.G. Vombatkere & Anr.

...Petitioners

Versus

Union of India & Ors.

...Respondents

AFFIDAVIT

I, I, Bezwada Wilson, S/o Late Shri Yacob, aged about 48 years,  
R/o 36/13 Ground Floor, East Patel Nagar, New Delhi, do hereby  
solemnly affirm and state as under:

1. I am the Petitioner No.2 herein, I am fully conversant with the facts  
and circumstances of the Present case and am as such competent to  
swear the present affidavit on behalf of the Petitioners.

2. I have read and understood the contents of the accompanying writ  
petition from pages 1849 through 1850; annexures thereto  
namely 1 through 4; the Synopsis and the List of  
Dates from pages 1849 through 1850 and say that the facts set out  
therein are true to my knowledge and submissions made therein are  
on legal advice received from my Advocates and believed to be true  
and correct and that the documents annexed are true copies of their  
respective originals.

  
DEPONENT

49

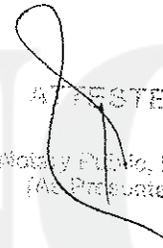
**VERIFICATION:**

Verified at Delhi on this 06th day of April, 2019 that the contents of paragraphs 1 to 2 of my above affidavit are true and correct to my knowledge, information and belief, that no part of it is false and nothing material has been concealed there from.

IDENTIFIED BY

  
DEPONENT



ATTESTED  
  
Notary P. P. Bansal, Delhi  
(As Presented)

06/04/19

—50—  
APPENDIX

जिस्ट्री सं० डी० एल०—(एन)04/0007/2003—19

REGISTERED NO. DL—(N)04/0007/2003—19



# भारत का राजपत्र The Gazette of India

असाधारण

EXTRAORDINARY

भाग II — खण्ड 1

PART II — Section 1

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं० 18] नई दिल्ली, शनिवार, मार्च 02, 2019/फाल्गुन 11, 1940 (सक)  
No. 18] NEW DELHI, SATURDAY, MARCH 02, 2019/PHALGUNA 11, 1940 (SAKA)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।  
Separate paging is given to this Part in order that it may be filed as a separate compilation.

MINISTRY OF LAW AND JUSTICE  
(Legislative Department)

New Delhi, the 2nd March, 2019/Phalgun 11, 1940 (Saka)

THE AADHAAR AND OTHER LAWS (AMENDMENT)  
ORDINANCE, 2019

NO 9 OF 2019

Promulgated by the President in the Seventieth Year of the Republic of India.

An Ordinance to amend the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and further to amend the Indian Telegraph Act, 1885 and the Prevention of Money-laundering Act, 2002.

WHEREAS the Aadhaar and Other Laws (Amendment) Bill, 2019 was passed by the House of the People on the 4<sup>th</sup> day of January, 2019 and is pending in the Council of States;

AND WHEREAS Parliament is not in session and the President is satisfied that circumstances exist which render it necessary for him to take immediate action;

NOW, THEREFORE, in exercise of the powers conferred by clause (1) of article 123 of the Constitution, the President is pleased to promulgate the following Ordinance:—

PART I  
PRELIMINARY

1.(1) This Ordinance may be called the Aadhaar and Other Laws (Amendment) Ordinance, 2019. Short title and commencement.

(2) It shall come into force at once.

- 51 -

PART II  
AMENDMENTS TO THE AADHAAR (TARGETED DELIVERY OF  
FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES)  
ACT, 2016

Amendment of  
section 2.

2. In section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereafter in this Part referred to as the principal Act),— 18 of 2016.

(i) for clause (a), the following clause shall be substituted, namely:—

‘(a) “Aadhaar number” means an identification number issued to an individual under sub-section (3) of section 3, and includes any alternative virtual identity generated under sub-section (4) of that section;’

(ii) after clause (a), the following clause shall be inserted, namely:—

‘(aa) “Aadhaar ecosystem” includes enrolling agencies, Registrars, requesting entities, offline verification-seeking entities and any other entity or group of entities as may be specified by regulations;’

(iii) after clause (b), the following clauses shall be inserted, namely:—

‘(ba) “Adjudicating Officer” means an adjudicating officer appointed under sub-section (1) of section 33B;

‘(bb) “Appellate Tribunal” means the Appellate Tribunal referred to in sub-section (1) of section 33C;’

(iv) after clause (i), the following clause shall be inserted, namely:—

‘(ia) “child” means a person who has not completed eighteen years of age;’

(v) after clause (p), the following clauses shall be inserted, namely:—

‘(pa) “offline verification” means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations;

‘(pb) “offline verification-seeking entity” means any entity desirous of undertaking offline verification of an Aadhaar number holder;’

Amendment of  
section 3.

3. In section 3 of the principal Act, after sub-section (3), the following sub-section shall be inserted, namely:—

“(4) The Aadhaar number issued to an individual under sub-section (3) shall be a twelve-digit identification number and any alternative virtual identity as an alternative to the actual Aadhaar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations.”

52

4. After section 3 of the principal Act, the following section shall be inserted, namely:—

Insertion of new section 3A.

“3A.(1) The enrolling agency shall, at the time of enrolment of a child, seek the consent of the parent or guardian of the child, and inform the parent or guardian, the details specified under sub-section (2) of section 3.

Aadhaar number of children.

(2) A child who is an Aadhaar number holder may, within a period of six months of attaining the eighteen years of age, make an application to the Authority for cancellation of his Aadhaar number, in such manner as may be specified by regulations and the Authority shall cancel his Aadhaar number.

(3) Notwithstanding anything in section 7, a child shall not be denied any subsidy, benefit or service under that section in case of failure to establish his identity by undergoing authentication, or furnishing proof of possession of Aadhaar number, or in the case of a child to whom no Aadhaar number has been assigned, producing an application for enrolment.”

5. In section 4 of the principal Act, for sub-section (3), the following sub-sections shall be substituted, namely:—

Amendment of section 4.

“(3) Every Aadhaar number holder to establish his identity, may voluntarily use his Aadhaar number in physical or electronic form by way of authentication or offline verification, or in such other form as may be notified, in such manner as may be specified by regulations.

*Explanation.*— For the purposes of this section, voluntary use of the Aadhaar number by way of authentication means the use of such Aadhaar number only with the informed consent of the Aadhaar number holder.

(4) An entity may be allowed to perform authentication, if the Authority is satisfied that the requesting entity is—

(a) compliant with such standards of privacy and security as may be specified by regulations; and

(b) (i) permitted to offer authentication services under the provisions of any other law made by Parliament; or

(ii) seeking authentication for such purpose, as the Central Government in consultation with the Authority, and in the interest of State, may prescribe.

(5) The Authority may, by regulations, decide whether a requesting entity shall be permitted the use of the actual Aadhaar number during authentication or only an alternative virtual identity.

(6) Every requesting entity to whom an authentication request is made by an Aadhaar number holder under sub-section (3) shall inform to the Aadhaar number holder of alternate and viable means of identification and shall not deny any service to him for refusing to, or being unable to, undergo authentication.

(7) Notwithstanding anything contained in the foregoing provisions, mandatory authentication of an Aadhaar number holder for the provision of

any service shall take place if such authentication is required by a law made by Parliament.”.

Amendment of section 8.

6. In section 8 of the principal Act,—

(a) in sub-section (2),—

(i) in clause (a), after the words “consent of an individual”, the words “, or in the case of a child obtain the consent of his parent or guardian” shall be inserted;

(ii) after clause (b), the following proviso shall be inserted, namely:—

“Provided that the requesting entity shall, in case of failure to authenticate due to illness, injury or infirmity owing to old age or otherwise or any technical or other reasons, provide such alternate and viable means of identification of the individual, as may be specified by regulations.”;

(b) in sub-section (3), after the words “for authentication”, the words “or in the case of a child, his parent or guardian” shall be inserted.

Insertion of new section 8A.

7. After section 8 of the principal Act, the following section shall be inserted, namely:—

Offline verification of Aadhaar number.

“8A.(1) Every offline verification of an Aadhaar number holder shall be performed in accordance with the provisions of this section.

(2) Every offline verification-seeking entity shall,—

(a) before performing offline verification, obtain the consent of an individual, or in the case of a child, his parent or guardian, in such manner as may be specified by regulations; and

(b) ensure that the demographic information or any other information collected from the individual for offline verification is only used for the purpose of such verification.

(3) An offline verification-seeking entity shall inform the individual undergoing offline verification, or in the case of a child, his parent or guardian the following details with respect to offline verification, in such manner as may be specified by regulations, namely:—

(a) the nature of information that may be shared upon offline verification;

(b) the uses to which the information received during offline verification may be put by the offline verification-seeking entity; and

(c) alternatives to submission of information requested for, if any.

(4) No offline verification-seeking entity shall—

(a) subject an Aadhaar number holder to authentication;

(b) collect, use, or store an Aadhaar number or biometric information of any individual for any purpose;

(c) take any action contrary to any obligation on it as may be specified by regulations.”.

8. For section 21 of the principal Act, the following section shall be substituted, namely:—

Substitution of new section for section 21.

“21.(1) The Authority shall appoint such officers and employees as may be required for the discharge of its functions under this Act.

Officers and other employees of Authority.

(2) The salaries and allowances payable to, and the other terms and conditions of service of, the officers and employees of the Authority shall be such as may be specified by regulations.”.

9. After section 23 of the principal Act, the following section shall be inserted, namely:—

Insertion of new section 23A.

“23A.(1) The Authority may for the discharge of its functions under this Act, or any rules or regulations made thereunder, by order, issue such directions from time to time to any entity in the Aadhaar ecosystem, as it may consider necessary.

Power of Authority to issue directions.

(2) Every direction issued under sub-section (1) shall be complied with by the entity in the Aadhaar ecosystem to whom such direction is issued.”.

10. For section 25 of the principal Act, the following section shall be substituted, namely:—

Substitution of new section for section 25.

“25.(1) There shall be constituted a Fund to be called the Unique Identification Authority of India Fund and there shall be credited thereto—

Fund.

(a) all grants, fees and charges received by the Authority under this Act; and

(b) all sums received by the Authority from such other sources as may be decided upon by the Central Government.

(2) The Fund shall be applied for meeting—

(a) the salaries and allowances payable to the Chairperson and members and administrative expenses including the salaries, allowances and pension payable to or in respect of officers and other employees of the Authority; and

(b) the expenses on objects and for purposes authorised by this Act.”.

11. In section 29 of the principal Act,—

Amendment of section 29.

(a) for sub-section (3), the following sub-section shall be substituted, namely:—

“(3) No identity information available with a requesting entity or offline verification-seeking entity shall be—

(a) used for any purpose, other than the purposes informed in writing to the individual at the time of submitting any information for authentication or offline verification; or

(b) disclosed for any purpose, other than purposes informed in writing to the individual at the time of submitting any information for authentication or offline verification:

Provided that the purposes under clauses (a) and (b) shall be in clear and precise language understandable to the individual.”;

(b) in sub-section (4), for the words “or core biometric information”, the words “, demographic information or photograph” shall be substituted.

Amendment of section 33.

12. In section 33 of the principal Act,—

(i) in sub-section (1),—

(a) for the words “District Judge”, the words “Judge of a High Court” shall be substituted;

(b) in the proviso, after the words “hearing to the Authority”, the words “and the concerned Aadhaar number holder” shall be inserted;

(c) after the proviso, the following proviso shall be inserted, namely:—

“Provided further that the core biometric information shall not be disclosed under this sub-section.”.

(ii) in sub-section (2), for the words “Joint Secretary”, the word “Secretary” shall be substituted.

Insertion of new Chapter VIA.

13. After Chapter VI of the principal Act, the following Chapter shall be inserted, namely:—

#### “CHAPTER VIA CIVIL PENALTIES

Penalty for failure to comply with provisions of this Act, rules, regulations and directions.

33A.(1) Where an entity in the Aadhaar ecosystem fails to comply with the provision of this Act, the rules or regulations made thereunder or directions issued by the Authority under section 23A, or fails to furnish any information, document, or return of report required by the Authority, such entity shall be liable to a civil penalty which may extend to one crore rupees for each contravention and in case of a continuing failure, with additional penalty which may extend to ten lakh rupees for every day during which the failure continues after the first contravention.

(2) The amount of any penalty imposed under this section, if not paid, may be recovered as if it were an arrear of land revenue.

Power to adjudicate.

33B.(1) For the purposes of adjudication under section 33A and imposing a penalty thereunder, the Authority shall appoint an officer of the Authority, who is not below the rank of a Joint Secretary to the Government of India and possessing such qualification and experience as may be

prescribed, to be an Adjudicating Officer for holding an inquiry in such manner as may be prescribed.

(2) No inquiry under sub-section (1) shall be initiated except by a complaint made by the Authority.

(3) While holding an inquiry, the Adjudicating Officer shall—

(a) provide the entity in the Aadhaar ecosystem against whom complaint is made, an opportunity of being heard;

(b) have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry.

(4) If the Adjudicating Officer, on such inquiry, is satisfied that the entity in the Aadhaar ecosystem has failed to comply with any provision of this Act or the rules or regulations made thereunder or directions issued by the Authority under section 23A, or has failed to furnish any information, document, or return of report required by the Authority, the Adjudicating Officer may, by order, impose such penalty under section 33A as he thinks fit.

33C.(1) The Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997, shall be Appellate Tribunal for the purposes of hearing appeals against the decision of the Adjudicating Officer under this Act.

Appeals to  
Appellate  
Tribunal.

24 of 1997.

(2) A person or entity in the Aadhaar ecosystem aggrieved by an order of the Adjudicating Officer under section 33B, may prefer an appeal to the Appellate Tribunal within a period of forty-five days from the date of receipt of the order appealed against, in such form and manner and accompanied with such fee as may be prescribed:

Provided that the Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(3) On receipt of an appeal under sub-section (2), the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(4) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the Adjudicating Officer.

(5) Any appeal filed under sub-section (2) shall be dealt with by the Appellate Tribunal as expeditiously as possible and every endeavour shall be made by it to dispose of the appeal within six months from the date on which it is presented to it.

(6) The Appellate Tribunal may, for the purpose of deciding an appeal before it, call for the records relevant to disposing of such appeal and make such orders as it thinks fit.

Procedure and powers of the Appellate Tribunal.

33D. The provisions of sections 14-I to 14K (both inclusive), 16 and 17 of the Telecom Regulatory Authority of India Act, 1997 shall, *mutatis mutandis*, apply to the Appellate Tribunal in the discharge of its functions under this Act, as they apply to it in the discharge of its functions under that Act. 24 of 1997.

Appeal to Supreme Court of India.

33E. (1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 or in any other law for the time being in force, an appeal shall lie against any order, not being an interlocutory order, of the Appellate Tribunal to the Supreme Court on any substantial question of law arising out of such order. 5 of 1908.

(2) No appeal shall lie against any decision or order made by the Appellate Tribunal which the parties have consented to.

(3) Every appeal under this section shall be preferred within a period of forty-five days from the date of the decision or order appealed against:

Provided that the Supreme Court may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

Civil court not to have jurisdiction.

33F. No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an Adjudicating Officer appointed under this Act or the Appellate Tribunal is empowered, by or under this Act to determine, and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act."

Amendment of section 38.

14. In section 38 of the principal Act, for the words "three years", the words "ten years" shall be substituted.

Amendment of section 39.

15. In section 39 of the principal Act, for the words "three years", the words "ten years" shall be substituted.

Substitution of new section for section 40.

16. For section 40 of the principal Act, the following section shall be substituted, namely:—

Penalty for unauthorised use by requesting entity or offline verification-seeking entity.

"40. Whoever,—

(a) being a requesting entity, uses the identity information of an individual in contravention of sub-section (2) of section 8; or

(b) being an offline verification-seeking entity, uses the identity information of an individual in contravention of sub-section (2) of section 8A,

shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both."

17. In section 42 of the principal Act, for the words "one year", the words "three years" shall be substituted. Amendment of section 42.

18. In section 47 of the principal Act, in sub-section (1), the following proviso shall be inserted, namely:— Amendment of section 47.

"Provided that the court may, on a complaint made by an Aadhaar number holder or individual take cognizance of any offence punishable under section 34 or 35 or 36 or 37 or 40 or section 41."

19. After section 50 of the principal Act, the following section shall be inserted, namely:— Insertion of new section 50A.

43 of 1961.

"50A. Notwithstanding anything contained in the Income Tax Act, 1961 or any other enactment for the time being in force relating to tax on income, profits or gains, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains." Exemption from tax on income.

20. In section 51 of the principal Act, for the words "Member, officer", the words "Member or officer" shall be substituted. Amendment of section 51.

21. In section 53 of the principal Act, in sub-section (2),—

Amendment of section 53.

(i) after clause (a), the following clause shall be inserted, namely:—

"(aa) the purpose for which the requesting entity may be allowed by the Authority to perform authentication under sub-clause (ii) of clause (b) of sub-section (4) of section 4;"

(ii) after clause (g), the following clauses shall be inserted, namely:—

"(ga) the qualification and experience of, and the manner of appointment of, the Adjudicating Officer under sub-section (1) of section 33B;

"(gb) the form, manner, and fee for an appeal to be filed under sub-section (2) of section 33C;"

22. In section 54 of the principal Act, in sub-section (2),—

Amendment of section 54.

(i) for clause (a), the following clause shall be substituted, namely:—

"(a) the entities or group of entities in the Aadhaar ecosystem under clause (aa), the biometric information under clause (g) and the demographic information under clause (k), the process of collecting demographic information and biometric information from the individuals by enrolling agencies under clause (m), and the modes of offline verification of Aadhaar number holder under clause (pa) of section 2;"

(ii) after clause (b), the following clauses shall be inserted, namely:—

"(ba) the manner of generating alternative virtual identity under sub-section (4) of section 3;

"(bb) the manner in which cancellation of an Aadhaar number may be carried out under sub-section (2) of section 3A;"

(iii) after clause (c), the following clauses shall be inserted, namely:—

“(ca) standards of privacy and security to be complied with by the requesting entities under sub-section (4) of section 4;

(cb) the classification of requesting entities under sub-section (5) of section 4;”;

(iv) after clause (f), the following clauses shall be inserted, namely:—

“(fa) the alternate and viable means of identification of individual under the proviso to clause (b) of sub-section (2) of section 8;

(fb) the manner of obtaining consent under clause (a) of sub-section (2), the manner of providing information to the individual undergoing offline verification under sub-section (3), and the obligations of offline verification-seeking entities under clause (c) of sub-section (4), of section 8A;”.

Omission of section 57.

23. Section 57 of the principal Act shall be omitted.

### PART III

#### AMENDMENT TO THE INDIAN TELEGRAPH ACT, 1885

Amendment of section 4 of Act 13 of 1885.

24. In section 4 of the Indian Telegraph Act, 1885, after sub-section (2), the following sub-sections shall be inserted, namely:—

(3) Any person who is granted a license under the first proviso to sub-section (1) to establish, maintain or work a telegraph within any part of India, shall identify any person to whom it provides its services by—

(a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or 18 of 2016.

(b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or 18 of 2016.

(c) use of passport issued under section 4 of the Passports Act, 1967; or 15 of 1967.

(d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf.

(4) If any person who is granted a license under the first proviso to sub-section (1) to establish, maintain or work a telegraph within any part of India is using authentication under clause (a) of sub-section (3) to identify any person to whom it provides its services, it shall make the other modes of identification under clauses (b) to (d) of sub-section (3) also available to such person.

(5) The use of modes of identification under sub-section (3) shall be a voluntary choice of the person who is sought to be identified and no person shall be denied any service for not having an Aadhaar number.

(6) If, for identification of a person, authentication under clause (a) of sub-section (3) is used, neither his core biometric information nor the Aadhaar number of the person shall be stored.

(7) Nothing contained in sub-sections (3), (4) and (5) shall prevent the Central Government from specifying further safeguards and conditions for compliance by any person who is granted a license under the first proviso to sub-section (1) in respect of identification of person to whom it provides its services.

*Explanation.*—The expressions “Aadhaar number” and “core biometric information” shall have the same meanings as are respectively assigned to them in clauses (a) and (j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

18 of 2016.

## PART IV

## AMENDMENT TO THE PREVENTION OF MONEY-LAUNDERING ACT, 2002

15 of 2002.

25. In chapter IV of the Prevention of Money-laundering Act, 2002 (hereafter in this Part, referred to as the principal Act), before section 12, the following section shall be inserted, namely:—

Insertion of new section 11A.

‘11A. (1) Every Reporting Entity shall verify the identity of its clients and the beneficial owner, by—

Verification of Identity by Reporting Entity.

18 of 2016.

(a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 if the reporting entity is a banking company; or

18 of 2016.

(b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or

15 of 1967.

(c) use of passport issued under section 4 of the Passports Act, 1967; or

(d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf.

18 of 2016.

Provided that the Central Government may, if satisfied that a reporting entity other than banking company, complies with such standards of privacy and security under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and it is necessary and expedient to do so, by notification, permit such entity to perform authentication under clause (a):

Provided further that no notification under the first proviso shall be issued without consultation with the Unique Identification Authority of India established under sub-section (1) of section 11 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the appropriate regulator.

18 of 2016.

61-

(2) If any reporting entity performs authentication under clause (a) of sub-section (1), to verify the identity of its client or the beneficial owner it shall make the other modes of identification under clauses (b), (c) and (d) of sub-section (1) also available to such client or the beneficial owner.

(3) The use of modes of identification under sub-section (1) shall be a voluntary choice of every client or beneficial owner who is sought to be identified and no client or beneficial owner shall be denied services for not having an Aadhaar number.

(4) If, for identification of a client or beneficial owner, authentication or offline verification under clause (a) or clause (b) of sub-section (1) is used, neither his core biometric information nor his Aadhaar number shall be stored.

(5) Nothing in this section shall prevent the Central Government from notifying additional safeguards on any reporting entity in respect of verification of the identity of its client or beneficial owner.

*Explanation.*— The expressions “Aadhaar number” and “core biometric information” shall have the same meanings as are respectively assigned to them in clauses (a) and (j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

18 of 2016.

Amendment of  
section 12.

26. In section 12 of the principal Act, in sub-section (1), clauses (c) and (d) shall be omitted.

Amendment of  
section 73.

27. In section 73 of the principal Act, in sub-section (2), clauses (j) and (jj) shall be omitted.

RAMNATH KOVIND,  
*President.*

DR. G. NARAYANA RAJU,  
*Secretary to the Govt. of India.*

62

**ANNEXURE P-1**

Petitioner No.1.1 i.e. Sudhir Vombatkere's profile.

The 1<sup>st</sup> Petitioner is a citizen of India and is aged about 71 years. The 1<sup>st</sup> Petitioner is a retired Indian Army officer who retired after 35 years in uniform in the rank of major general from the post of Additional DG in charge of Discipline and Vigilance at Army HQ, New Delhi. He has been awarded the Visishta Seva Medal (VSM) by President of India in 1993 for his distinguished service rendered in Ladakh.

He holds a PhD degree in civil structural dynamics from I.I.T., Madras. After retirement, he is engaged in voluntary social work as Mysore and other areas around Karnataka. The 1<sup>st</sup> Petitioner is also an Adjunct Associate Professor in International Studies of the University of Iowa, USA and teaches under graduate students from USA and Canada in programs where the students visit Mysore.

In so far as the Unique Identification Project UID project") is concerned, the 1<sup>st</sup> Petitioner has written various articles pointing out the security risks of the project.

63-

## **ANNEXURE P-2**

### **PROFILE OF MR. BEZWADA WILSON**

- He is one of the founders and the National Convener of the Safai Karmachari Andolan, a human rights organization that has been campaigning for the eradication of manual scavenging and the emancipation of people employed for the purpose of manual scavenging.
- He was also the convener of the sub-group on safai karmacharis constituted by the Planning Commission of India.
- In 2009, he was chosen as the "Ashoka Senior Fellow" of human rights.
- By virtue of being the founder of Safai Karmachari Andolan, he was also actively involved in a public interest litigation before this Hon'ble Court in Writ Petition (Civil) No. 583 of 2003, Safai Karmachari Andolan and Ors. v. Union of India & Ors. The subject matter of that petition is strict implementation of the Employment of Manual Scavengers and Construction of Dry Latrines (Prohibition) Act, 1993.
- The Planning Commission of India constituted a sub-group on safai karmacharis with Mr. Wilson as its convener.
- In the year 2016, he received the prestigious Ramon Magsaysay Award.

64 -

ANNEXURE P-3

रजिस्ट्री सं० डी० एल—(एन)04/0007/2003—19

REGISTERED NO. DL—(N)04/0007/2003—19



**भारत का राजपत्र**  
**The Gazette of India**

असाधारण

EXTRAORDINARY

भाग II—खण्ड 1

PART II—Section I

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं० 18] नई दिल्ली, शनिवार, मार्च 02, 2019/फाल्गुन 11, 1940 (साक)  
No. 18] NEW DELHI, SATURDAY, MARCH 02, 2019/PHALGUNA 11, 1940 (SAKA)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।  
Separate paging is given to this Part in order that it may be filed as a separate compilation.

MINISTRY OF LAW AND JUSTICE  
(Legislative Department)

New Delhi, the 2nd March, 2019/Phalguna 11, 1940 (Saka)

THE AADHAAR AND OTHER LAWS (AMENDMENT)  
ORDINANCE, 2019

No 9 OF 2019

Promulgated by the President in the Seventieth Year of the Republic of India.

An Ordinance to amend the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and further to amend the Indian Telegraph Act, 1885 and the Prevention of Money-laundering Act, 2002.

WHEREAS the Aadhaar and Other Laws (Amendment) Bill, 2019 was passed by the House of the People on the 4<sup>th</sup> day of January, 2019 and is pending in the Council of States;

AND WHEREAS Parliament is not in session and the President is satisfied that circumstances exist which render it necessary for him to take immediate action;

NOW, THEREFORE, in exercise of the powers conferred by clause (1) of article 123 of the Constitution, the President is pleased to promulgate the following Ordinance:—

PART I  
PRELIMINARY

1.(1) This Ordinance may be called the Aadhaar and Other Laws (Amendment) Ordinance, 2019.

Short title and commencement.

(2) It shall come into force at once.

65

2

THE GAZETTE OF INDIA EXTRAORDINARY

[PART II—

PART II  
AMENDMENTS TO THE AADHAAR (TARGETED DELIVERY OF  
FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES)  
ACT, 2016

Amendment of  
section 2.

2. In section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereafter in this Part referred to as the principal Act),—

18 of 2016.

(i) for clause (a), the following clause shall be substituted, namely:—

‘(a) “Aadhaar number” means an identification number issued to an individual under sub-section (3) of section 3, and includes any alternative virtual identity generated under sub-section (4) of that section;’

(ii) after clause (a), the following clause shall be inserted, namely:—

‘(aa) “Aadhaar ecosystem” includes enrolling agencies, Registrars, requesting entities, offline verification-seeking entities and any other entity or group of entities as may be specified by regulations;’

(iii) after clause (b), the following clauses shall be inserted, namely:—

‘(ba) “Adjudicating Officer” means an adjudicating officer appointed under sub-section (1) of section 33B;

‘(bb) “Appellate Tribunal” means the Appellate Tribunal referred to in sub-section (1) of section 33C;’

(iv) after clause (i), the following clause shall be inserted, namely:—

‘(ia) “child” means a person who has not completed eighteen years of age;’

(v) after clause (p), the following clauses shall be inserted, namely:—

‘(pa) “offline verification” means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations;

‘(pb) “offline verification-seeking entity” means any entity desirous of undertaking offline verification of an Aadhaar number holder;’

Amendment of  
section 3.

3. In section 3 of the principal Act, after sub-section (3), the following sub-section shall be inserted, namely:—

“(4) The Aadhaar number issued to an individual under sub-section (3) shall be a twelve-digit identification number and any alternative virtual identity as an alternative to the actual Aadhaar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations.”

66 -

4. After section 3 of the principal Act, the following section shall be inserted, namely:—

Insertion of new section 3A.

“3A.(1) The enrolling agency shall, at the time of enrolment of a child, seek the consent of the parent or guardian of the child, and inform the parent or guardian, the details specified under sub-section (2) of section 3.

Aadhaar number of children.

(2) A child who is an Aadhaar number holder may, within a period of six months of attaining the eighteen years of age, make an application to the Authority for cancellation of his Aadhaar number, in such manner as may be specified by regulations and the Authority shall cancel his Aadhaar number.

(3) Notwithstanding anything in section 7, a child shall not be denied any subsidy, benefit or service under that section in case of failure to establish his identity by undergoing authentication, or furnishing proof of possession of Aadhaar number, or in the case of a child to whom no Aadhaar number has been assigned, producing an application for enrolment.”

5. In section 4 of the principal Act, for sub-section (3), the following sub-sections shall be substituted, namely:—

Amendment of section 4.

“(3) Every Aadhaar number holder to establish his identity, may voluntarily use his Aadhaar number in physical or electronic form by way of authentication or offline verification, or in such other form as may be notified, in such manner as may be specified by regulations.

*Explanation.*— For the purposes of this section, voluntary use of the Aadhaar number by way of authentication means the use of such Aadhaar number only with the informed consent of the Aadhaar number holder.

(4) An entity may be allowed to perform authentication, if the Authority is satisfied that the requesting entity is—

(a) compliant with such standards of privacy and security as may be specified by regulations; and

(b) (i) permitted to offer authentication services under the provisions of any other law made by Parliament; or

(ii) seeking authentication for such purpose, as the Central Government in consultation with the Authority, and in the interest of State, may prescribe.

(5) The Authority may, by regulations, decide whether a requesting entity shall be permitted the use of the actual Aadhaar number during authentication or only an alternative virtual identity.

(6) Every requesting entity to whom an authentication request is made by an Aadhaar number holder under sub-section (3) shall inform to the Aadhaar number holder of alternate and viable means of identification and shall not deny any service to him for refusing to, or being unable to, undergo authentication.

(7) Notwithstanding anything contained in the foregoing provisions, mandatory authentication of an Aadhaar number holder for the provision of

67

any service shall take place if such authentication is required by a law made by Parliament.”

Amendment of section 8.

6. In section 8 of the principal Act,—

(a) in sub-section (2),—

(i) in clause (a), after the words “consent of an individual”, the words “, or in the case of a child obtain the consent of his parent or guardian” shall be inserted;

(ii) after clause (b), the following proviso shall be inserted, namely:—

“Provided that the requesting entity shall, in case of failure to authenticate due to illness, injury or infirmity owing to old age or otherwise or any technical or other reasons, provide such alternate and viable means of identification of the individual, as may be specified by regulations.”;

(b) in sub-section (3), after the words “for authentication,”, the words “or in the case of a child, his parent or guardian” shall be inserted.

Insertion of new section 8A.

7. After section 8 of the principal Act, the following section shall be inserted, namely:—

Offline verification of Aadhaar number.

“8A.(1) Every offline verification of an Aadhaar number holder shall be performed in accordance with the provisions of this section.

(2) Every offline verification-seeking entity shall,—

(a) before performing offline verification, obtain the consent of an individual, or in the case of a child, his parent or guardian, in such manner as may be specified by regulations; and

(b) ensure that the demographic information or any other information collected from the individual for offline verification is only used for the purpose of such verification.

(3) An offline verification-seeking entity shall inform the individual undergoing offline verification, or in the case of a child, his parent or guardian the following details with respect to offline verification, in such manner as may be specified by regulations, namely:—

(a) the nature of information that may be shared upon offline verification;

(b) the uses to which the information received during offline verification may be put by the offline verification-seeking entity; and

(c) alternatives to submission of information requested for, if any.

(4) No offline verification-seeking entity shall—

(a) subject an Aadhaar number holder to authentication;

68-

Sec. 1]

THE GAZETTE OF INDIA EXTRAORDINARY

5

(b) collect, use, or store an Aadhaar number or biometric information of any individual for any purpose;

(c) take any action contrary to any obligation on it as may be specified by regulations.”.

8. For section 21 of the principal Act, the following section shall be substituted, namely:—

Substitution of new section for section 21.

“21.(1) The Authority shall appoint such officers and employees as may be required for the discharge of its functions under this Act.

Officers and other employees of Authority.

(2) The salaries and allowances payable to, and the other terms and conditions of service of, the officers and employees of the Authority shall be such as may be specified by regulations.”.

9. After section 23 of the principal Act, the following section shall be inserted, namely:—

Insertion of new section 23A.

“23A.(1) The Authority may for the discharge of its functions under this Act, or any rules or regulations made thereunder, by order, issue such directions from time to time to any entity in the Aadhaar ecosystem, as it may consider necessary.

Power of Authority to issue directions.

(2) Every direction issued under sub-section (1) shall be complied with by the entity in the Aadhaar ecosystem to whom such direction is issued.”.

10. For section 25 of the principal Act, the following section shall be substituted, namely:—

Substitution of new section for section 25.

“25.(1) There shall be constituted a Fund to be called the Unique Identification Authority of India Fund and there shall be credited thereto—

Fund.

(a) all grants, fees and charges received by the Authority under this Act; and

(b) all sums received by the Authority from such other sources as may be decided upon by the Central Government.

(2) The Fund shall be applied for meeting—

(a) the salaries and allowances payable to the Chairperson and members and administrative expenses including the salaries, allowances and pension payable to or in respect of officers and other employees of the Authority; and

(b) the expenses on objects and for purposes authorised by this Act.”.

11. In section 29 of the principal Act,—

Amendment of section 29.

(a) for sub-section (3), the following sub-section shall be substituted, namely:—

“(3) No identity information available with a requesting entity or offline verification-seeking entity shall be—

(a) used for any purpose, other than the purposes informed in writing to the individual at the time of submitting any information for authentication or offline verification; or

(b) disclosed for any purpose, other than purposes informed in writing to the individual at the time of submitting any information for authentication or offline verification:

Provided that the purposes under clauses (a) and (b) shall be in clear and precise language understandable to the individual.”;

(b) in sub-section (4), for the words “or core biometric information”, the words “, demographic information or photograph” shall be substituted.

Amendment of section 33.

12. In section 33 of the principal Act,—

(i) in sub-section (1),—

(a) for the words “District Judge”, the words “Judge of a High Court” shall be substituted;

(b) in the proviso, after the words “hearing to the Authority”, the words “and the concerned Aadhaar number holder” shall be inserted;

(c) after the proviso, the following proviso shall be inserted, namely:—

“Provided further that the core biometric information shall not be disclosed under this sub-section.”.

(ii) in sub-section (2), for the words “Joint Secretary”, the word “Secretary” shall be substituted.

Insertion of new Chapter VIA.

13. After Chapter VI of the principal Act, the following Chapter shall be inserted, namely:—

#### “CHAPTER VIA CIVIL PENALTIES

Penalty for failure to comply with provisions of this Act, rules, regulations and directions.

33A.(1) Where an entity in the Aadhaar ecosystem fails to comply with the provision of this Act, the rules or regulations made thereunder or directions issued by the Authority under section 23A, or fails to furnish any information, document, or return of report required by the Authority, such entity shall be liable to a civil penalty which may extend to one crore rupees for each contravention and in case of a continuing failure, with additional penalty which may extend to ten lakh rupees for every day during which the failure continues after the first contravention.

(2) The amount of any penalty imposed under this section, if not paid, may be recovered as if it were an arrear of land revenue.

Power to adjudicate.

33B.(1) For the purposes of adjudication under section 33A and imposing a penalty thereunder, the Authority shall appoint an officer of the Authority, who is not below the rank of a Joint Secretary to the Government of India and possessing such qualification and experience as may be

70

prescribed, to be an Adjudicating Officer for holding an inquiry in such manner as may be prescribed.

(2) No inquiry under sub-section (1) shall be initiated except by a complaint made by the Authority.

(3) While holding an inquiry, the Adjudicating Officer shall—

(a) provide the entity in the Aadhaar ecosystem against whom complaint is made, an opportunity of being heard;

(b) have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry.

(4) If the Adjudicating Officer, on such inquiry, is satisfied that the entity in the Aadhaar ecosystem has failed to comply with any provision of this Act or the rules or regulations made thereunder or directions issued by the Authority under section 23A, or has failed to furnish any information, document, or return of report required by the Authority, the Adjudicating Officer may, by order, impose such penalty under section 33A as he thinks fit.

33C.(1) The Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997, shall be Appellate Tribunal for the purposes of hearing appeals against the decision of the Adjudicating Officer under this Act.

Appeals to  
Appellate  
Tribunal.

24 of 1997.

(2) A person or entity in the Aadhaar ecosystem aggrieved by an order of the Adjudicating Officer under section 33B, may prefer an appeal to the Appellate Tribunal within a period of forty-five days from the date of receipt of the order appealed against, in such form and manner and accompanied with such fee as may be prescribed:

Provided that the Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(3) On receipt of an appeal under sub-section (2), the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(4) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the Adjudicating Officer.

(5) Any appeal filed under sub-section (2) shall be dealt with by the Appellate Tribunal as expeditiously as possible and every endeavour shall be made by it to dispose of the appeal within six months from the date on which it is presented to it.

shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both."

section 8A,  
(b) being an offline verification-seeking entity, uses the identity information of an individual in contravention of sub-section (2) of

(a) being a requesting entity, uses the identity information of an individual in contravention of sub-section (2) of section 8; or

"40. Wherever,—

16. For section 40 of the principal Act, the following section shall be substituted, namely:—

15. In section 39 of the principal Act, for the words "three years", the words "ten years" shall be substituted.

14. In section 38 of the principal Act, for the words "three years", the words "ten years" shall be substituted.

33F. No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an Adjudicating Officer appointed under this Act or the Appellate Tribunal is empowered, by or under this Act to determine, and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act."

Provided that the Supreme Court may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(3) Every appeal under this section shall be preferred within a period of forty-five days from the date of the decision or order appealed against:

(2) No appeal shall lie against any decision or order made by the Appellate Tribunal which the parties have consented to.

out of such order.

shall lie against any order, not being an interlocutory order, of the Appellate Tribunal to the Supreme Court on any substantial question of law arising

Procedure, 1908 or in any other law for the time being in force, an appeal shall lie against anything contained in the Code of Civil

33E. (1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 or in any other law for the time being in force, an appeal shall lie against anything contained in the Code of Civil

33D. The provisions of sections 14-1 to 14K (both inclusive), 16 and 17 of the Telecom Regulatory Authority of India Act, 1997 shall, *mutatis mutandis*, apply to the Appellate Tribunal in the discharge of its functions under this Act, as they apply to it in the discharge of its functions under that Act.

(6) The Appellate Tribunal may, for the purpose of deciding an appeal before it, call for the records relevant to disposing of such appeal and make such orders as it thinks fit.

#

Civil court not to have jurisdiction.  
Amendment of section 38.  
Amendment of section 39.  
Substitution of new section for section 40.  
Penalty for unauthorized use by requesting entity or offline verification-seeking entity.

Procedure and powers of the Appellate Tribunal.  
Appeal to Supreme Court of India.

72

Sec. 1]

THE GAZETTE OF INDIA EXTRAORDINARY

9

17. In section 42 of the principal Act, for the words "one year", the words "three years" shall be substituted. Amendment of section 42.

18. In section 47 of the principal Act, in sub-section (1), the following proviso shall be inserted, namely:— Amendment of section 47.

"Provided that the court may, on a complaint made by an Aadhaar number holder or individual take cognizance of any offence punishable under section 34 or 35 or 36 or 37 or 40 or section 41."

19. After section 50 of the principal Act, the following section shall be inserted, namely:— Insertion of new section 50A.

43 of 1961.

"50A. Notwithstanding anything contained in the Income Tax Act, 1961 or any other enactment for the time being in force relating to tax on income, profits or gains, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains."

Exemption from tax on income.

20. In section 51 of the principal Act, for the words "Member, officer", the words "Member or officer" shall be substituted. Amendment of section 51.

21. In section 53 of the principal Act, in sub-section (2),— Amendment of section 53.

(i) after clause (a), the following clause shall be inserted, namely:—

"(aa) the purpose for which the requesting entity may be allowed by the Authority to perform authentication under sub-clause (ii) of clause (b) of sub-section (4) of section 4;"

(ii) after clause (g), the following clauses shall be inserted, namely:—

"(ga) the qualification and experience of, and the manner of appointment of, the Adjudicating Officer under sub-section (1) of section 33B;

(gb) the form, manner, and fee for an appeal to be filed under sub-section (2) of section 33C."

22. In section 54 of the principal Act, in sub-section (2),— Amendment of section 54.

(i) for clause (a), the following clause shall be substituted, namely:—

"(a) the entities or group of entities in the Aadhaar ecosystem under clause (aa), the biometric information under clause (g) and the demographic information under clause (k), the process of collecting demographic information and biometric information from the individuals by enrolling agencies under clause (m), and the modes of offline verification of Aadhaar number holder under clause (pa) of section 2;"

(ii) after clause (b), the following clauses shall be inserted, namely:—

"(ba) the manner of generating alternative virtual identity under sub-section (4) of section 3;

(bb) the manner in which cancellation of an Aadhaar number may be carried out under sub-section (2) of section 3A."

73

(iii) after clause (c), the following clauses shall be inserted, namely:—

“(ca) standards of privacy and security to be complied with by the requesting entities under sub-section (4) of section 4;

(cb) the classification of requesting entities under sub-section (5) of section 4;”;

(iv) after clause (f), the following clauses shall be inserted, namely:—

“(fa) the alternate and viable means of identification of individual under the proviso to clause (b) of sub-section (2) of section 8;

(fb) the manner of obtaining consent under clause (a) of sub-section (2), the manner of providing information to the individual undergoing offline verification under sub-section (3), and the obligations of offline verification-seeking entities under clause (c) of sub-section (4), of section 8A;”.

Omission of section 57.

23. Section 57 of the principal Act shall be omitted.

### PART III

#### AMENDMENT TO THE INDIAN TELEGRAPH ACT, 1885

Amendment of section 4 of Act 13 of 1885.

24. In section 4 of the Indian Telegraph Act, 1885, after sub-section (2), the following sub-sections shall be inserted, namely:—

“(3) Any person who is granted a license under the first proviso to sub-section (1) to establish, maintain or work a telegraph within any part of India, shall identify any person to whom it provides its services by—

(a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or 18 of 2016.

(b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or 18 of 2016.

(c) use of passport issued under section 4 of the Passports Act, 1967; or 15 of 1967.

(d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf.

(4) If any person who is granted a license under the first proviso to sub-section (1) to establish, maintain or work a telegraph within any part of India is using authentication under clause (a) of sub-section (3) to identify any person to whom it provides its services, it shall make the other modes of identification under clauses (b) to (d) of sub-section (3) also available to such person.

(5) The use of modes of identification under sub-section (3) shall be a voluntary choice of the person who is sought to be identified and no person shall be denied any service for not having an Aadhaar number.

74

(6) If, for identification of a person, authentication under clause (a) of sub-section (3) is used, neither his core biometric information nor the Aadhaar number of the person shall be stored.

(7) Nothing contained in sub-sections (3), (4) and (5) shall prevent the Central Government from specifying further safeguards and conditions for compliance by any person who is granted a license under the first proviso to sub-section (1) in respect of identification of person to whom it provides its services.

*Explanation.*—The expressions “Aadhaar number” and “core biometric information” shall have the same meanings as are respectively assigned to them in clauses (a) and (j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

18 of 2016.

PART IV

AMENDMENT TO THE PREVENTION OF MONEY-LAUNDERING ACT, 2002

15 of 2002.

25. In chapter IV of the Prevention of Money-laundering Act, 2002 (hereafter in this Part, referred to as the principal Act), before section 12, the following section shall be inserted, namely:—

Insertion of new section 11A.

‘11A. (1) Every Reporting Entity shall verify the identity of its clients and the beneficial owner, by—

Verification of identity by Reporting Entity.

18 of 2016.

(a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 if the reporting entity is a banking company; or

18 of 2016.

(b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or

15 of 1967.

(c) use of passport issued under section 4 of the Passports Act, 1967; or

(d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf.

18 of 2016.

Provided that the Central Government may, if satisfied that a reporting entity other than banking company, complies with such standards of privacy and security under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and it is necessary and expedient to do so, by notification, permit such entity to perform authentication under clause (a):

Provided further that no notification under the first proviso shall be issued without consultation with the Unique Identification Authority of India established under sub-section (1) of section 11 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the appropriate regulator.

18 of 2016.

75

(2) If any reporting entity performs authentication under clause (a) of sub-section (1), to verify the identity of its client or the beneficial owner it shall make the other modes of identification under clauses (b), (c) and (d) of sub-section (1) also available to such client or the beneficial owner.

(3) The use of modes of identification under sub-section (1) shall be a voluntary choice of every client or beneficial owner who is sought to be identified and no client or beneficial owner shall be denied services for not having an Aadhaar number.

(4) If, for identification of a client or beneficial owner, authentication or offline verification under clause (a) or clause (b) of sub-section (1) is used, neither his core biometric information nor his Aadhaar number shall be stored.

(5) Nothing in this section shall prevent the Central Government from notifying additional safeguards on any reporting entity in respect of verification of the identity of its client or beneficial owner.

*Explanation.*— The expressions “Aadhaar number” and “core biometric information” shall have the same meanings as are respectively assigned to them in clauses (a) and (j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

18 of 2016.

Amendment of  
section 12.

26. In section 12 of the principal Act, in sub-section (1), clauses (c) and (d) shall be omitted.

Amendment of  
section 73.

27. In section 73 of the principal Act, in sub-section (2), clauses (j) and (jj) shall be omitted.

RAM NATH KOVIND,  
*President.*

DR. G. NARAYANA RAJU,  
*Secretary to the Govt. of India.*

FB

ANNEXURE P- 4

रजिस्ट्री सं० डी० एल०-33004/99

REGD. NO. D. L.-33004/99



# भारत का राजपत्र The Gazette of India

असाधारण  
EXTRAORDINARY  
भाग III—खण्ड 4  
PART III—Section 4

प्राधिकार से प्रकाशित  
PUBLISHED BY AUTHORITY

सं. 90] नई दिल्ली, बृहस्पतिवार, मार्च 7, 2019/फाल्गुन 16, 1940  
No. 90] NEW DELHI, THURSDAY, MARCH 7, 2019/PHALGUNA 16, 1940

भारतीय विशिष्ट पहचान प्राधिकरण  
अधिसूचना  
नई दिल्ली, 6 मार्च, 2019

आधार (अधिप्रमाणन सेवाओं का मूल्य-निर्धारण) विनियम, 2019

(2019 का संख्या 1)

सं. के-11022/632/2019/अधि-यूआईडीएआई (2019 का संख्या 1) — आधार (वित्तीय और अन्य सहायिकियों और सेवाओं का लक्षित परिधान) अधिनियम, 2016 की धारा 8 के साथ पठित धारा 54 के उप-नियम (1) तथा उप-नियम (2) के उप-खंड (एफ) और आधार (अधिप्रमाणन) विनियम, 2016 के विनियम 12(7) में प्रदत्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण, एतद्वारा निम्नलिखित विनियम बनाता है, नामतः:

- संक्षिप्त नाम और प्रारंभ:-
  - इन विनियमों को आधार (अधिप्रमाणन सेवाओं का मूल्य-निर्धारण) विनियम, 2019 (2019 का संख्या 1) कहा जाएगा।
  - ये विनियम सरकारी राजपत्र में प्रकाशन की तिथि से लागू होंगे।
- आधार अधिप्रमाणन सेवाओं का मूल्य-निर्धारण:-
  - प्रत्येक ई-केवाईसी कार्यसम्पादन के लिए 20 रुपए (कर सहित) की दर से और अनुरोधकर्ता संस्था से प्रत्येक हां/नहीं कार्यसम्पादन के लिए 0.50 रुपए (कर सहित) की दर से आधार अधिप्रमाणन सेवाओं का प्रभार वसूला जाएगा;
  - सरकारी संस्थाएं और डाक विभाग को अधिप्रमाणन कार्यसम्पादन प्रभारों से छूट होगी; तथा
  - दिनांक 14 जुलाई, 2017 की राजपत्र अधिसूचना सं. 13012/79/2017/विधि-यूआईडीएआई (2017 का संख्या 4) के अनुसार आधार नामांकन और अद्यतन सुविधाएं प्रदान करने में कार्यरत अधिसूचित व्यावसायिक दैकों को अधिप्रमाणन कार्यसम्पादन प्रभारों से छूट

77

2

THE GAZETTE OF INDIA : EXTRAORDINARY

[PART III—SEC. 4]

होगी। हालांकि, ऐसे बैंक, जो आधार नामांकन और अद्यतन लक्ष्यों, समय-समय पर यथा संप्रेषित, को पूरा नहीं कर पाते हैं, से लक्ष्य की प्राप्ति में हुई कमी के अनुपात में प्रभार वसूला जाएगा।

- (4) उपरोक्त प्रभार, लाइसेंस शुल्क और वित्तीय हतोत्साहन, यथा लागू, के अतिरिक्त होंगे।  
 (5) कार्यसम्पादन त्रुटि कोडों एवं उससे सम्बंधित प्रभारों का ब्योरा अलग से जारी किया जाएगा।

**3. अधिप्रमाणन और ई-केवाईसी सेवाओं की अनिर्ंतरता:-**

(1) यदि कोई विद्यमान अनुरोधकर्ता संस्था [उपरोक्त 2(2) और 2(3) विनियमों में दी गयी छूट को छोड़कर], इन विनियमों के प्रकाशन के तिथि के बाद आधार अधिप्रमाणन की सेवाओं का उपयोग जारी रखता है तो, यह समझा जाएगा कि वह निर्दिष्ट अधिप्रमाणन प्रभारों के प्रति सहमत है। संस्थाओं को उपयोग पर आधारित संबंधित बीजक (इनवोइस) जारी होने के 15 दिनों के अंतर्गत अधिप्रमाणन कार्यसम्पादन प्रभारों को जमा करना अपेक्षित होगा। 15 दिनों की अवधि के बाद भुगतान में विलंब होने पर, 1.5% प्रतिमाह की दर से चक्रवृद्धि ब्याज अदा करना होगा तथा अधिप्रमाणन एवं ई-केवाईसी सेवाएं भी रोक दी जाएंगी।

(2) यदि कोई अनुरोधकर्ता संस्था अधिप्रमाणन कार्यसम्पादन के प्रभारों का भुगतान नहीं करना चाहता है, तो वह आधार अधिप्रमाणन सेवाओं के उपयोग को बंद कर देगी और वह अपने निर्णय से तुरंत यूआईडीएआई को सूचित करेगी, और वह आधार (अधिप्रमाणन) विनियम, 2016 के विनियम 23 के अनुसार अधिप्रमाणन सुविधाओं को ऐक्सेस करने का परित्याग कर देगी। हालांकि, अधिप्रमाणन सेवाओं के ऐक्सेस के निष्क्रिय होने की तिथि तक लागू कार्यसम्पादन प्रभारों का भुगतान करना होगा।

डॉ. अजय भूषण पाण्डेय, मुख्य कार्यकारी अधिकारी

[ विज्ञापन-III/4/ असा./566/18 ]

THE UNIQUE IDENTIFICATION AUTHORITY OF INDIA  
 NOTIFICATION

New Delhi, the 6th March, 2019

AADHAAR (PRICING OF AADHAAR AUTHENTICATION SERVICES) REGULATIONS, 2019

(No. 1 of 2019)

No.K-11022/632/2019/Auth-UIDAI (No. 1 of 2019).—In exercise of the powers conferred by sub-section (1) and sub-clause (f) of sub-section (2) of Section 54 read with Section 8 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and Regulation 12(7) of the Aadhaar (Authentication) Regulations, 2016, the Unique Identification Authority of India hereby makes the following regulations, namely:—

**1. Short title and commencement.—**

(1) These regulations may be called the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 (No. 1 of 2019).

(2) These shall come into force from the date of their publication in the Official Gazette.

**2. Pricing of Aadhaar Authentication Services.—**

(1) Aadhaar authentication services shall be charged @ Rs 20 (including taxes) for each e-KYC transaction and Rs 0.50 (including taxes) for each Yes/No authentication transaction from requesting entities;

(2) Government entities and the Department of Posts shall be exempt from Authentication transaction charges; and

(3) Scheduled Commercial Banks engaged in providing Aadhaar enrolment and update facilities in accordance with Gazette Notification no. 13012/79/2017/Legal-UIDAI (No 4 of 2017) dated 14<sup>th</sup> July 2017 shall be exempt from Authentication transaction charges. However, such banks, which fall short of the Aadhaar enrolment and update targets, as communicated from time to time, will be charged in proportion to the shortfall in achieving the target.

(4) The above charges shall be in addition to the License fees and financial disincentives, as applicable.

(5) Details of the transaction error codes and its charges shall be issued separately.

78

3. Discontinuation of authentication and e-KYC services.—

(1) If an existing requesting entity [except those exempt under Regulations 2(2) and 2(3) above], continues to use Aadhaar authentication services beyond the date of publication of these Regulations, it shall be deemed to have agreed to the specified authentication charges. The entities shall be required to deposit the authentication transaction charges within 15 days of issuance of the concerned invoice based on the usage. The delay in payment beyond 15 days shall attract interest compounded @ 1.5% per month and discontinuation of authentication and e-KYC services.

(2) In case a requesting entity does not wish to pay authentication transaction charges, it shall discontinue the use of Aadhaar authentication services and intimate its decision to the UIDAI immediately, and it shall surrender its access to the authentication facilities as per Regulation 23 of the Aadhaar (Authentication) Regulations, 2016. However, the transaction charges as applicable till the date of de-activation of access to authentication services shall have to be paid.

Dr. AJAY BHUSHAN PANDEY, Chief Executive Officer

[ ADVT.-III/4/Exty./566/18 ]

BAR & BENCH

TRUE COPY

ANNEXURE P- 5

JK

IN THE SUPREME COURT OF INDIA  
CIVIL ORIGINAL JURISDICTION  
WRIT PETITION (CIVIL) \_\_\_\_ OF 2019

IN THE MATTER OF:

S.G. VOMBATKERE & ANR

...PETITIONERS

Versus

UNION OF INDIA & ANR

...RESPONDENTS

AFFIDAVIT

I, Samir Kelekar s/o Gurunath Kelekar, aged about 55 years and resident of # 210, 1 st Floor, 3<sup>rd</sup> B Cross, Domlur Layout, Bangalore 560071 hereby solemnly affirm and declare that :-

1. That this Affidavit is to reaffirm the contents of the Affidavit dt. 06.04.2016 (hereinafter, "the Earlier Affidavit") in relation to and for the purposes of explaining the clear possibility of surveillance of Aadhaar holder that exists with the Aadhaar/UID system.
2. That a true copy of the Earlier Affidavit is annexed herewith and marked as ANNEXURE-A-1.
3. That I hereby reiterate and reaffirm the statements of facts as stated in the Earlier Affidavit, particularly from Paras 1 through 13, except to the extent that the details in relation to my residential address and occupation have now changed and that I presently reside at the address mentioned above and work as the the team lead of security & Chief Technology Officer, Advanced Technology Group, Cisco India Ltd.
4. That I am aware that this Affidavit may be placed on record of the Hon'ble Supreme Court India in the captioned Writ Petition that *inter*



80

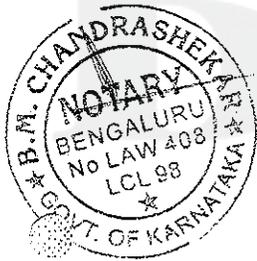
aliachallenges the Constitutional Validity of the Aadhaar & Other Laws  
Amendment Ordinance, 2019.

*Sanjay Kelaka*  
DEPONENT

**VERIFICATION**

Verified at Bengaluru on \_\_\_\_\_ that the contents of the above  
affidavit from Paras 1 through 4 are true to the best of my knowledge and  
belief, no part thereof is false and that nothing material is concealed  
therefrom.

*Sanjay Kelaka*  
DEPONENT



SWORN TO BEFORE ME  
*B.M. Chandrashekar*  
B.M. CHANDRASHEKAR  
Advocate & Notary Public  
B D.A. Complex, Koramangala  
BANGALORE - 560 034  
Mob 9689103253

CL No. 818 Page No. 76  
BOOK No. XXX DATE 2/4/19

81-

**AFFIDAVIT**

I, Samir Kelekar s/o Gurunath Kelekar, aged about 53 years and resident of # 337, 2<sup>nd</sup> Floor, Amar Jyothi Layout, Domlur Layout, Bangalore 560071 hereby solemnly affirm and declare that :-

1. That I have working experience of more than thirty (30) years in the field of IT and about 15 years of experience in the field of cyber security and that currently I am heading a company which I founded for the purpose of providing security solutions to organisations which need to protect themselves against Internet / Cyber / digital frauds.
2. That my firm's name is M/s. Teknotrends Software Pvt. Ltd.
3. That I graduated in electrical engineering from the Indian Institute, Mumbai (IIT, Mumbai) in 1983. Thereafter I obtained a post-graduate degree in Computer Engineering from Clemson University, South Carolina, USA.
4. That I hold a doctorate degree (PhD) in electrical engineering from Columbia University, New York, USA.
5. That I have done work for clients, including, Canara Bank, G E Health and MTN, a multi-national South African mobile phone company.
6. That I am aware that the Government of India is implementing "UID / Aadhaar" based authentication for various government services and that private entities may also use the UID / "Aadhaar" database for identifying individuals.
7. That I am aware that there are petitions before the Hon'ble

82

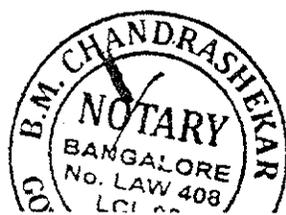
to be placed by one or more of the petitioners in support of their challenge on the said grounds to the said project.

8. That as someone with fairly extensive experience of cyber security, I can categorically state that this project is highly imprudent, as it throws open the clear possibility of compromising basic privacy by 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 said authority or authentication data traffic as the case may be.
9. That I state that I have perused the documents that UIDAI have put out in relation to the design of the Aadhaar authentication system, and I can categorically state that it is quite easy to know the place and type of transaction every time such authentication takes place using a scanner for fingerprints or iris and the records of these in the UID / "Aadhaar" database. Knowing the various types of transactions done via a particular aadhar number would help UIDAI or related parties to track the behaviour of a person using Aadhar.
10. I state that biometric scanners also have IP Addresses and these IP addresses can be used to locate the place ( city or town) from where the transaction took place. Any administrator of the UIDAI server or any employee or other person with access to transaction data, with a little help from the servers (Authentication User Agents and Authentication Server Agents, as they are called in UIDAI literature), through which authentication request is sent to the UIDAI, will be able to track the transaction and the person carrying out the same. Further, I also point out that UIDAI recommends that each point of service device i.e. the device from which an authentication request

83

and being able to map every authentication transaction to be emanating from a unique registered device, further makes the task of tracking down the place from which an authentication request emanates easier.

11. I further state that there are technical tools that are available that make it easy and possible to track the electronic path that authentication requests from any given authentication device to the Central Identification Data Repository take as part of their authentication transaction.
12. I further wish to point out that today, it is well known that no security is perfect. The idea is to design a system where in in case of a breach, the damage is minimal and backups are available. Hence, passwords should be changeable. Biometrics as a password is problematic in that it cannot be changed if stolen / lost / hacked.
13. That secondly, a centralized database has the problem that once hacked all data can be lost. Specifically, consider if the Army personnel use this as an authentication mechanism before getting their salaries. The place from which they authenticate can be found as it will be done via a scanner which has an IP address / is on a mobile internet. This data will be available in the logs of the Aadhaar system or the logs of the intermediate servers. A compromise of the system having the above details means that the hackers can know the place of each army personnel of the country at the time when they take their salary. This can be a big risk to national security, and this is just one example as to why it is, in my opinion, imprudent to use such a system.



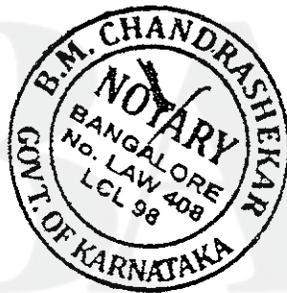
*Sanjay Madhukar*  
DEPONENT

84-

true and correct to the best of my knowledge and nothing material is concealed therefrom.

Verified on sixth (6<sup>th</sup>) day of April 2016.

*Sanghulika*  
DEPONENT



SWORN TO BEFORE ME

*Sanghulika*  
B.M. CHANDRASHEKAR  
Advocate & Notary Public  
# 5, BDA Complex, Koramangala,  
BENGALURU - 560 034  
Mob: 9448104253

BAR & BENCH



महाराष्ट्र MAHARASHTRA

2019

UX 551522

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) \_\_\_\_\_ OF 2019

पधान मुद्रांक कार्यालय, मुंबई  
प.म. नि. क्र. १.००००२०  
22 MAR 2019  
सक्षम अधिकारी

श्रीमती. पी. एस. तळेकर

IN THE MATTER OF:

S.G. VOMBATKERE & ANR

... PETITIONERS

VERSUS

UNION OF INDIA & ANR

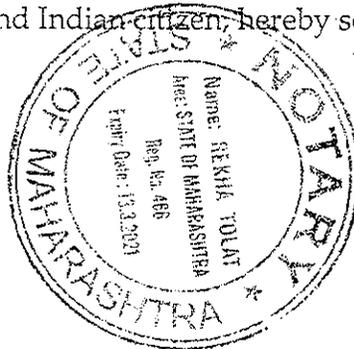
... RESPONDENTS

AFFIDAVIT

I, Jude Terrence D' Souza resident of 16, Lovely Society, Sector 2, Airoli,

Navi Mumbai 400 708, and Indian citizen, hereby solemnly affirm and

declare that:-



86

1. That this Affidavit is to reaffirm the contents of the Affidavit dt. 04.11.2016 (hereinafter, "the Earlier Affidavit") in relation to and for the purposes of explaining the clear possibility of surveillance of Aadhaar holder that exists with the Aadhaar/UID system.
2. That a true copy of the Earlier Affidavit is annexed herewith and marked as ANNEXURE-A-1.
3. That I hereby reiterate and reaffirm the statements of facts as stated in the Earlier Affidavit.
4. That I am aware that this Affidavit may be placed on record of the Hon'ble Supreme Court India in the captioned Writ Petition that *inter alia* challenges the Constitutional Validity of the Aadhaar & Other Laws Amendment Ordinance, 2019.

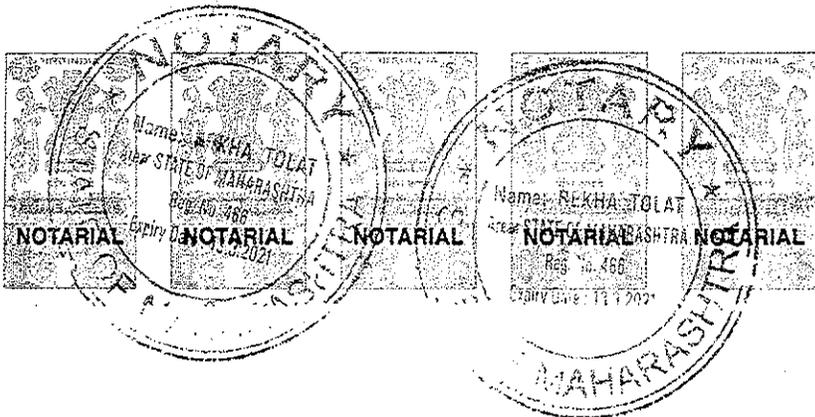


J.T. D'Souza

DEPONENT  
BEFORE ME

*[Signature]* 11/11/19

NOTARY  
MAHARASHTRA STATE  
S.M. 9818



**TOLAT & CO.**  
MISS. REKHA A. TOLAT, ADVI  
Yesur Building, Lot Over Shop A  
Ground Floor, 43, M. G. Road  
Mumbai - 400 001.

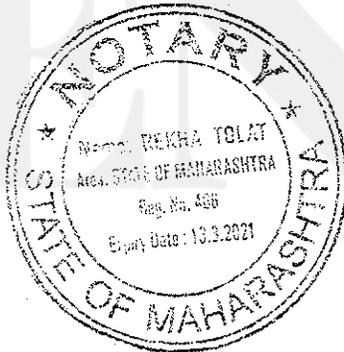
87

VERIFICATION

Verified at Mumbai on 11<sup>th</sup> April 2019 that the contents of the above affidavit from Paras 1 to 2 are true to the best of my knowledge and belief, no part thereof is false and that nothing material is concealed therefrom.

J.T. D'SOUZA

DEPONENT



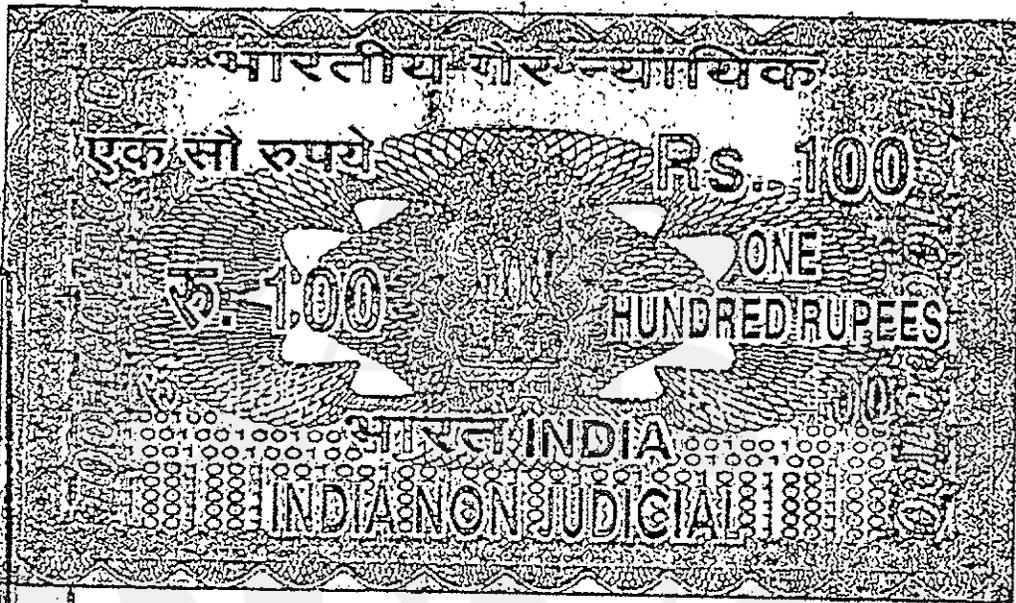
BEFORE ME

*[Signature]* 11/4/19

NOTARY  
MAHARASHTRA STATE

88

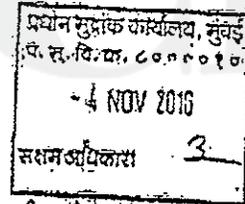
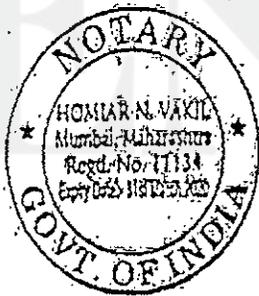
11



MAHARASHTRA

2016

RP 477141



I, Jude Terrence D'souza, Mumbai Indian inhabitant residing at 16, Lovely Society, Sector 3, Airoli, Navj Mumbai 400 708 do on solemn affirmation state as follows:

I am a securities system specialist. Due to the sensitivity of my work and this case I am not naming my present employer. However, I am willing to place the name and address of my present employer in

89

2

12

sealed envelope to be handed over to the Hon'ble Supreme Court, if required. Prior to my present work and position, I was employed with Bee Electronic Machines Ltd. and was engaged in office automation and telecommunications.

cc D/Sd  
2018

2. I have experience of around 35 years working with respect to electronic and embedded systems and I have developed a specialisation with regard to security features in relation to products and services provided by diverse companies. In the course of my present employment, I personally and my company (of which I am the Managing Director) have provided our services to well known and multi-national and national companies including the Reserve Bank of India, ICICI Bank, H. Dipak & Company (engaged in the diamond industry), Rosyblu India (also engaged in the diamond industry), etc.



3. I have studied the procedure and working of the Aadhaar program and have conducted demonstrations to show the unreliability of finger print authentication. At one of my demonstrations held at Bangalore in 2010, officers who were involved in the UIDAI / Aadhaar program were also present and witnessed the ease with which finger prints can be replicated and misused for the purposes of 'authentication'.

90

3

13

4. As a concerned citizen and at the request of the writ petitioners in this case, I have agreed to demonstrate to the Learned Judges of this Hon'ble Court the ease with which finger prints can be replicated using material available in the market.

5. In addition, I would like to make the following points which have a bearing on this case and support the grounds in the petition:

(a) The Aadhaar authentication is carried out by a device commonly known as a finger print reader. Each of these finger print readers is required to have a GPS device built within it, in terms of the specifications prescribed by the UIDAI. The acronym GPS stands for Global Positioning System and GPS employs satellite based technology to pin point a location. The accuracy of GPS devices enables location to within a radius of around 10-20 metres. In other words, signals emanating from a GPS device when processed can enable a person to fix the location of that device.

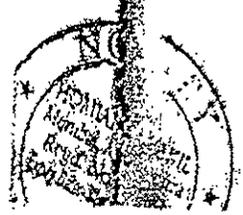
(b) Every finger print reader also has a unique identification number peculiar to that finger print reader / device alone. The specifications also state that each device may have a pincode.

91

4

14

- (c) Whenever an authentication of a finger print is required through the Aadhaar verification process, the finger print reader communicates electronically with the server(s) maintained by the UIDAI which is a central depository of biometric information. At the time of each and every request for authentication / verification, the finger print reader is required to electronically indicate its unique identification number to the central depository server. Combining the unique number of the finger print reader with the in-built GPS, the location of the individual whose finger print is being verified becomes known, virtually in real time. The verification system is so designed that it can operate as a real time surveillance system of every individual who is required to give his / her finger print for the purpose of authentication.
- (d) As the Aadhaar verification system is used progressively in more and more applications, the extent and pervasiveness of the surveillance will increase.
- (e) By way of illustration, if Aadhaar verification using a finger print reader is carried out at say an airport for boarding an aircraft or at a public distribution shop for collecting rations or for withdrawing money from an automatic teller at a bank.



92

5

15'

(ATM), the state will know the precise location of the individual.

(f) Even if the GPS system is disabled, since the finger print reader is communicating with the central depository through an electronic connection, it is easily possible to locate the finger print reader and in that manner, the place where the individual seeking verification is located.

(g) I have personally examined more than one finger print readers by opening the casing of these machines. Between the capture of the finger print and the processor that carries out encryption, there is a connection that can be easily tampered with to capture the biometric data *before encryption* in a separate device known in the trade as 'skimmers'. The reason I make this point is that it is easily possible for an enrolling agency or the authenticating body (both of whom have finger print readers) to duplicate and capture the biometrics before the point of encryption.

(h) My experience in working with diverse types of electronic hardware, computers and a variety of devices that work on what are generally known as 'computers' compels me to make an additional point with respect to the security and safety of the data stored with the central depository and other servers in the

93

6

16

UIDAI network. There are several levels of computer language known as 'codes' that are embedded in computers and devices. In so far as I am aware, the devices employed by the UIDAI for registration and authentication of biometrics are not indigenously manufactured and are manufactured by or sourced through overseas corporations. The source code, machine code, etc. which are fundamental in operating the hardware and software utilised by UIDAI, are not known to or owned by the UIDAI but are the proprietary, confidential information belonging to third parties including overseas corporations. It is possible that the codes and the software have hidden or concealed features that are called 'Backdoor' and 'Trojan' features that enable mining, removal and use of so called encrypted data without anyone including UIDAI realising. Further within the microcontrollers used on these devices it is definitely possible to have hardware backdoors, which would be nearly impossible to identify. I emphasise this point because it had national security dimensions of a magnitude that cannot be exaggerated. Backdoor or Trojan mining could enable third parties access to all or part of the information in the central depository and servers maintained by UIDAI. This information at a future date could be misused by persons having



94

17

interest inimical to those of India for commercial or political gain.

- (i) Apart from surveillance, the matter data of individuals collected over lifetime could be a most potent 'weapon' or 'tool' for black mail, exploitation and political gain. Illustratively, if Aadhaar authentication becomes ubiquitous (as UIDAI would like) in a few years time, the profile of every political functionary, bureaucrat, judge, captain of industry, professional will be known. This would amount to a complete compromise of privacy of not only lay individuals and citizens but also of important constitutional functionaries.

6. Although I have tried to express myself in simple terms, I am ready and willing to remain present before this Hon'ble Court in the course of the hearing and explain the points in this affidavit in addition to the demonstration I have referred to earlier in this affidavit.
7. Although, I have not personally carried out any specific test in respect of iris recognition, on the basis of my experience in the field of security systems, I say that using modern photography instruments including cameras embedded as features in high end phones, it is easily possible to replicate irises and use these false iris copies for the purposes of authentication.





96

## ANNEXURE P-7

Indian Institute of Technology Kanpur  
Directorate

Manindra Agrawal  
Officiating Director

### **Analysis of Major Concerns about Aadhar Privacy and Security**

Manindra Agrawal, IIT Kanpur

Aadhar is a mechanism to provide a unique ID to every resident of India. It is similar to mechanisms implemented in several countries (e.g., Social Security Number in US), but also different in one crucial way; it uses biometric data of an individual for verification in addition to other factors. This additional information allows for a more secure way of establishing identity of a resident, however, several concerns have been raised about privacy and security of the mechanism. In this write up, I analyze the major ones.

In real world, at any time, a large number of mechanisms (referred to as protocols in the security literature) are in the play simultaneously. Hence at times, it is not straightforward to identify the protocol that is causing a reduction in security or privacy. To address this, the notion of differential privacy and differential security are used. Differential privacy of a protocol is the change in the privacy of people when the protocol is introduced without altering any other protocol present. Similarly, differential security of a protocol is the change in the security of people when the protocol is introduced without altering any other protocol present. If the differential privacy of a protocol is non-negative, the protocol does not compromise privacy in any way. Similarly for differential security of a protocol.

97

I will analyze differential privacy and differential security of Aadhar protocol. There are three major arguments articulated against Aadhar (referred to as attacks in the security literature).

1. Surveillance Attack : If Aadhar is used to establish the identify of an individual everywhere state can used the access data to Aadhar database of an individual to track him/her.
2. Forgery Attack: By capturing the fingerprint of person X anyone can impersonate X
3. Database Attack: If the Aadhar database gets hacked biometric information of all residents of the country is compromised.

It is clear that the first attack compromises privacy of an individual, while the latter two compromise security. Hence, one is tempted to conclude that Aadhar protocol suffers from these drawbacks. However, in order to be certain, let us analyze the differential privacy and security of the Aadhaar protocol with respect to these attacks.

#### Surveillance Attack

This attack can only take place under a state that does not go by the law. This is because the Aadhar Act explicitly prohibits use of Aadhar data for any purpose except for ID verification. Let us assume India becomes such a state. Further, suppose Aadhar protocol is absent. An individual would then use alternative mechanisms to verify his/her identity at various places. Most of these places are already connected to internet (banks, airport etc.) and if not connected, the personal information can be called upon from the various agencies by the state under the various laws. Therefore the totalitarian state can ask ISPs to provide all the packet data to it, or call upon various agencies and departments for personal information and thereby track an

98

individual completely. The only way to avoid this would be when an individual forgoes his rights and does not go to any place where his/her identity needs to be established. However, in that case, even in presence of Aadhar protocol the individual cannot be tracked.

Therefore, the differential privacy of Aadhar with respect to Surveillance Attack is non-negative.

#### Forgery Attack

Let us suppose person Y has been able to obtain fingerprint of person X. In Aadhar protocol, fingerprint has to be presented before an authorized receiver to an authorized device for ID validation. There are two ways in which security of person X can get compromised. One authorized receiver is hand-in-glove with Y and allows the fingerprint of X to be entered into the device. Second, Y puts of an artificial skin layer on his thumb that has X's fingerprint and fools the receiver. Now suppose Aadhar protocol is not present. Person Y can forge other ID of X (PAN Card, Driving License etc) with roughly the same effort as fingerprint. Now, any place ID of X is to be presented. Y can use the forged ID. One situation that stands out as exception is the use of signature in large money transactions (more than Rs.50,000), where the correctness of signature is carefully checked. This case is not applicable to Aadhar protocol since it is not used for large money transaction.

Therefore, the differential security of Aadhar with respect to Forgery Attack is non-negative.

#### Database Attack

There exist four Aadhar databases:

99

1. Person Database stores personal attributes of a person (name, address, age etc) along with his/her Aadhar number.
2. Reference Database stores Aadhar number of a person along with a unique reference number (which has no relationship with Aadhar number of an individual).
3. Biometric Database stores biometric information of a person along with the unique reference number.
4. Verification Log records of ID verifications done in the past five years. For each verification, it stores the biometric data, Aadhar number, and ID of the device on which the verification was done.

The Biometric Database is accessible by third-party vendors providing biometric search and deduplication algorithms. The other three databases are stored in encrypted form by UIDAI. Let us analyze the situation where one of the first three databases gets leaked. The first point to note is that all the databases are stored in encrypted form so a mere leak does not provide any information – one also needs decryption key. Let us assume that decryption key is also leaked. The only way a database can get misused is to forge identity of a set of persons, say  $X_1, X_2, X_3, \dots, X_n$ . In order to do this, one needs to associate with personal attributes and Aadhar number of person  $X_j$  his/her fingerprints. Note that none of the three databases individually provide association of fingerprints with personal attributes and Aadhar number of any individual. Hence to create association of  $X_j$  with his/her fingerprints, one needs to either access both Biometric Database and Reference Database, or track person  $X_j$  to obtain his/her fingerprints and validate them from the Reference Database. In the later case, there is no need for Reference Database for forging the identity. Hence, the security can

100

only get affected when at least Biometric and Reference Databases are leaked.

So if the Reference database is secure, the other two databases can be made public, and the differential security with respect to Forgery Attack would still be non-negative

Let us analyze the case when the Reference Database also gets leaked. This allows one to forge identities of all residents of the country. Although the simple Forgery Attack will still have non-negative differential security, now one can launch a different form of Forgery Attack continuously change forged identities. This is not possible without access to this database. Hence, differential security of this attack is negative. Therefore, Reference database must be kept secure.

Finally, let us turn attention to verification Log. Its leakage may affect both the security and the privacy of an individual as one can extract identities of several people (and hence can keep changing forged identities) and also locate the places of transactions done by an individual in the past five years. Note that differential privacy of this becomes negative since without access to this database it is not possible to track locations of an individual in past five years (as opposed to tracking current location which is possible). Therefore, Verification Log must be kept secure.

The above arguments show that leakage of Reference Database or Verifications Log compromises security or privacy, and one may be tempted to argue against Aadhar protocol on this basis. However, this is not so. Let us carefully analyze what we have argued. We have shown that both the databases must be kept secure, unlike other databases that can be made

101

public without compromising security. Assume that a lot of care is taken to keep both the databases secure. It is still possible that, with significant effort, one may be able to break their security. Now assume Aadhar protocol is absent. We would still have databases of other IDs, eg., PAN card database, driving licence database etc. With same effort as required to break the security of Aadhar databases, one can break these databases as well and then forge IDs of multiple people. Hence, assuming Reference Databases and Verification Log are kept secure, their differential security is non-negative.

In a similar vein, breach of Verification Log results in leakage of approximate locations of an individual where he/she did ID verification in the past five years. In the absence of Aadhar protocol, with a similar amount of effort, one can breach other databases (bank transactions, SIM registration etc.) and extract approximate locations of an individual. Moreover, breaking into Aadhar databases is a criminal offence, and hence is likely to deter most such attempts. Hence, assuming Verification Log is kept secure, its differential privacy is non-negative.

#### Conclusions

As analyzed above, none of the listed attacks on Aadhar protocol compromise privacy or security. There is an overall reduction of privacy and security, but that is due to movement of society into digital world and internet and not because of Aadhar protocol. The societies have despite reduction in security and privacy wholeheartedly adopted these technologies as there are significant advantages. Specifically with respect to Aadhar protocol, it brings significant benefits to our society, without any further

102

reduction in security and privacy as long as it is ensured that the key databases are extremely hard to penetrate.

If required, I will be happy to depose before the court on the above analysis.

Sd/-  
Manindra Agrawal  
N Rama Rao Professor  
Department of Computer Science and Engineering  
IIT Kanpur

BAR &  
BENCH  
//TRUE COPY//

103

Annexure P-2 (Colly.)

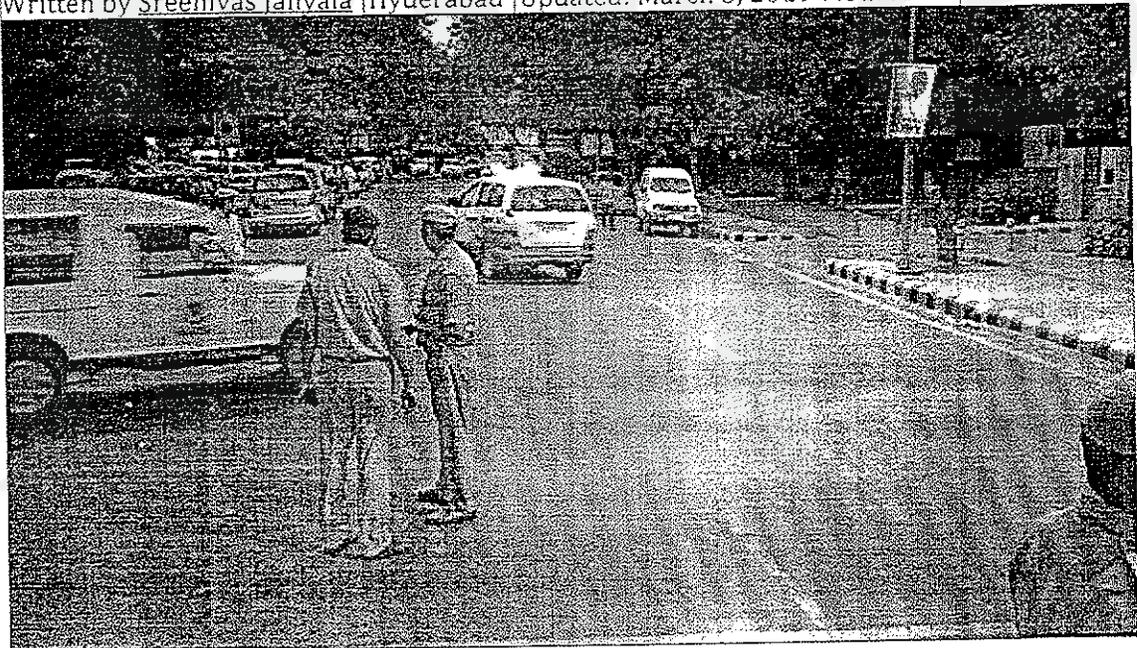
ANNEXURE P-8

## Indian Express

# IT firm working on app for TDP 'stole' data of Andhra voters, say cops

The Hyderabad-based firm, IT Grids India Pvt Ltd, was hired by the ruling Telugu Desam Party (TDP) in Andhra Pradesh to develop an app for use in the forthcoming elections - the state is bound for Assembly polls as well this summer.

Written by Sreenivas Janvala |Hyderabad |Updated: March 5, 2019 7:51:46 am



The police suspect IT Grids either stole the database or was provided the data by a Visakhapatnam-based IT company that works for AP government. (Representational image)

The probe into alleged misuse of data for voter profiling in Andhra Pradesh by an IT firm has found that the company got information and sensitive data of people related to Aadhaar, electoral rolls, government scheme

beneficiaries, and voter's information, according to Cyberabad Police, which is investigating the case.

The Hyderabad-based firm, IT Grids India Pvt Ltd, was hired by the ruling Telugu Desam Party (TDP) in Andhra Pradesh to develop an app for use in the forthcoming elections – the state is bound for Assembly polls as well this summer.

The police suspect IT Grids either stole the database or was provided the data by a Visakhapatnam-based IT company that works for AP government.

The issue has sparked a war of words between political parties in AP and Telangana. While TDP has alleged that Telangana Police is harassing IT Grids, which is developing apps for the party, and accused ruling TRS in Telangana of helping YSR Congress, TDP's main opposition in AP, YSR Congress leaders have lodged a complaint against AP Police officials who came to question Lokeshwara Reddy, a data analyst whose complaint led Cyberabad Police to file a case on March 2.

On Monday, Cyberabad Police Commissioner V C Sajjanar said, "IT Grids India also runs the 'Sevamitra' app application of TDP. Through this, they have constituency-wise voter data and voters' party-wise affiliation. They have an option to identify preference of a voter for a particular party."

He said the app has details such as voter ID, caste and addresses.

Officials said they conducted raids at offices of IT Grids on March 3 and 4 and seized electronic gadgets, computer hard discs, mobile phones and written documents, among others.

Sajjanar said, "We have learnt that 45-50 cases have been registered in various places of AP about deletion of voters by police on the Election Commission of India's (EC) direction. We have issued a notice to Amazon Web Services for production of database relating to application and other

Annexure P-2 (Colly.)

105

data (the database is said to have been stored with Amazon Web Services, a subsidiary of the US-headquartered Amazon). We are also writing to UIDAI and EC for more details.”

AP Chief Electoral Officer Krishna Dwivedi said he received complaints that anonymous applications to delete some voters' names were being sent to election officials. “I have asked district collectors (concerned) to register complaints, if this is true. Voters' names cannot be deleted without verification by election officials, but we will look into these complaints,” Dwivedi said.

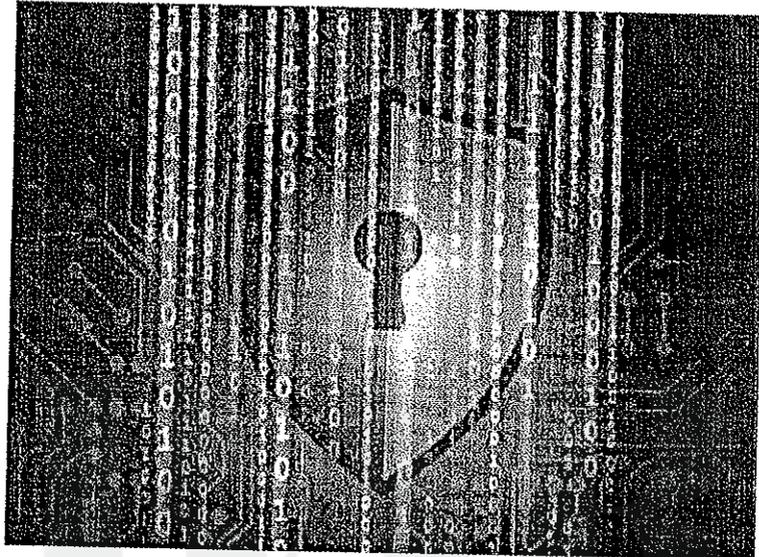
Link: <https://indianexpress.com/article/india/it-firm-working-on-app-for-tdp-stole-data-of-andhra-voters-say-cops-5611073/#comments>

BAR &  
BENCH

TIMES OF INDIA

## Andhra Pradesh: TDP app breached data of 3.7cr voters? Probe begins

TNN | Feb 26, 2019, 06.43 AM IST



HYDERABAD: A massive probe has been launched by multiple agencies such as Unique Identification Authority of India, Election Commission of India and Cyberabad police into a complaint filed regarding alleged privacy breach and misuse of data of 3.7 crore voters in Andhra Pradesh.

The complaint was filed by YSR Congress MP V Vijaysai Reddy against Hyderabad-based IT Grids (India) Pvt Ltd's 'Sevamitra' app promoting the Telugu Desam Party (TDP). Vijaysai alleged that government data from the Smart Pulse Survey which was linked to State Resident Data Hub (SRDH) containing demographic data of Aadhaar and electoral rolls prepared by the ECI were misused.

IT Grids India Pvt Limited, based in Madhapur, has done several applications and other IT solutions for various AP government departments and is also the developer of the ruling TDP 'Sevamitra' app.

The app has voter ID numbers, names, colour photos, booth-level information, family details, caste information and government schemes and amounts a voter gets as beneficiary. The app comes with all the information inbuilt and is extensively used by TDP activists.

20/03/2019

Andhra Pradesh: TDP app breached data of 3.7cr voters? Probe begins - Times of India

107

Investigators are now focusing on how the company obtained family details and beneficiary data. Cyberabad police commissioner V C Sajjanar told TOI, "We have received the complaint and are yet to register an FIR. We are studying the contents."

EC should regulate breach of privacy: Security researcher

An e-mail and messages sent to the promoter of IT Grid went unanswered. Sources said Ashok Dakavaram told police that the data used in the app is collected from open data sources available on electoral rolls and the survey conducted house-to-house by the party workers. He denied collecting any information from Aadhaar or SRDH or any government database.

Security researcher Srinivas Kodali told TOI, "Any personal information of a voter is part of his fundamental right of privacy. The Election Commission needs to regulate any breach." On June 19, 2018, TOI published a story on the breach of data of 4.5 crore citizens from Smart Pulse Survey after Kodali exposed it.

An Election Commission official told TOI, "The soft copy of electoral rolls provided to political parties is only non-photo electoral roll data. The hard copy printouts are given in black and white with photos. We haven't supplied any soft copy or hard copy of electoral rolls to any party or any company."

Officials of UIDAI are yet to respond on whether the photographs and family grouping belongs to their database or SRDH. An official of UIDAI said, "We have asked the states to destroy SRDH after a Supreme Court judgement. We were informed that Andhra Pradesh destroyed it a few months ago. But we have to verify whether Smart Pulse survey database is still having traces and demographic details collected from SRDH."

Andhra Pradesh government created an SRDH in association with UIDAI and the SRDH mirror image of the Aadhaar data

20/03/2019

Andhra Pradesh: TDP app breached data of 3.7cr voters? Probe begins - Times of India

108

relating to AP from the Data Repository of UIDAI in Bengaluru. SRDH contains the basic data like a resident's Aadhaar number, name, date of birth or year of birth, gender, address, postal pin code, photo, biometric data.

In 2016, the AP government took up Smart Pulse Survey of all households, aimed at capturing socio-economic data directly in digital form, with online validations. It is aimed at completing the seeding of Aadhaar with departments' database, ensuring correctness of data already seeded with Aadhaar, e-string the demographic data in the SRDH.

AP Government information technology advisor J Satyanarayana, who is also chairman of UIDAI, told TOI, "The Smart Pulse Survey is integration and convergence of the multiple databases of socioeconomic data of the people with the SRDH database. The purpose is for real-time governance and aimed at checking whether the welfare schemes are reaching beneficiaries. SRDH as a separate entity has been stopped."

109

**ANNEXURE P-10**

**FIRST INFORMATION REPORT**  
(Under Sections 154 and 157 Cr.P.C.)

A.P.P.M. Orders 470,500

1. District : Cyberabad P.S. Madhapur (Guttala) Year 2019 Fir No. 174/2019  
Date 02.03.2019
2. Act & Sections(s) : 120b, 379, 420, 188 IPC, 72, 66-B ITA-2000-2008
3. (a) Occurrence of offence: Day: Saturday Date & Time from  
Date & time to : Prior To: 02/03/2019 00:15 Time period : 0  
(b) Information received at P.S. Date & Time: 02.03.2019 00:15  
(c) General Diary Reference : Entry No:12 Date & Time: 02.03.2019 00:15
4. Type of Information : Written
5. Place of occurrence  
(a) Distance and Direction from PS.: 3 Km, North-West Beat No.  
Beat Madhapur  
(b) Address Place : Area/Mandal: Street/Village:  
Plot No. 538, 5<sup>th</sup> Floor, Krishna Serilingampally Khanamet, Madhapur  
Heights, Ayyappa Society State: Telangana PIN:  
(c) In case, outside the limits of the police station , then  
Name of the P.S. -- District ---
6. Complainant/Informant:  
(a) Name Sri Thummala Lokeswara Reddy  
(b) Father's/Husband's Name: Thummala Nagamllia Reddy  
(c) Date/Year of Birth Age : 40  
(d) Nationality : Indian (e) Caste:  
(f) Passport No: Date of issue: Place of issue:  
(g) Occupation Data Analyst Mobile No:  
(h) Address House No: Area/Mandal: Street/Village  
Villa No.17, Orchids Indu Hyderabad Hyderabad  
Fortune, Fields, 13<sup>th</sup> Phase
7. Details of known/suspected/unknown accused with full particulars:  
Serial No.: 1  
a) Name: Management of MS IT GRIDS India Pvt. Ltd. and others  
b) Father's/Husband's Name: (c) Occupation:  
d) Caste: e) Gender: Male f) Age: Nationality:  
Management of M/s IT GRIDS

110

g) (Inida) Pvt. Ltd. Street/Village Area/Mandal:  
 City/District: state PIN:  
 h) Phone(Off): 0 Phone(Resi): 0 Cell No.:0

Physical features, deformities and other details of the Suspect:

S.No.	Sex	Date/Year of Birth	Build	Height(ems)	Complexion	Identification Marks(s)
1	2	3	4	5	6	7
1	Male	DOB/AGE:0		Ocm		

Deformalities/ Peculiarities	Teeth	Hair	Eyes	Habbits(s)	Dress Habit(s)	Languages/Dialect
					1	

Place Of				
Burn Mark	Leucoderma	Mole	Scar	Illegible
15	16	17	18	Illegible

8. Reasons for delay in reporting by the complainant/informant  
 Delay due to the complainant for through research as specified in the enclosures
9. Particulars of properties stolen/involved (Attach separate sheet, if necessary)
10. Total value of property stolen:
11. Inquest Report/U.D. Case No. If any ---
12. Contents of the complaint/statement of the complainant or informant:

IN THE COURT OF HONOURABLE XII ADL. METROPOLITAN MAGISTRATE,  
 KUKATPALLY, CYBERABAD

Honoured sir,

Today i.e., on 02.03.2019 at 0015 hours received a petition from Sri Thummala Lokeswara Reddy S/o Thummala Nagamalla Reddy, aged 40 years, Occ: Data Analyst, R/o Villa No.17, Orchids, Indu Fortune Fields, 13<sup>th</sup> Phase, Hyderabad, Cell NO. 9642499116. Which reads as follows.

The brief facts of the case are that on 02.03.2019 at 00.15 hours received a complaint from Thummala Lokeswara Reddy, R/o Villa No.17, Indu Fortune Fields, Hyderabad that while studying about the practices of electioneering in view of the upcoming general elections, 2019 in Andhra Pradesh he learnt about the use of certain mobile phone and tab based software applications by the cadre of Telugu Desam Party (TDP) especially 'Sevamitra app' for advancing party's electoral prospects as reported in the National Newspaper. When browsed the website of TDP i.e., w.w.w.telugudesam.org and the

111

official Facebook page of Telugu Desam Party, the details of "Sevamitra app" is available which was meant for people who were registered as TDP members to gather information about voters and to work for the party's win the elections in 2019. It came to know from the study of "Sevamitra app" that Govt of AP utilized the services of M/s. Bluefrog Mobile Technologies Pvt. Ltd, Visakhapatnam in the implementation of Govt schemes and functions of AP. during the course of discharge of works by Bluefrog Ltd is was given access to enormous amount of official data in respect of the beneficiaries of various Government schemes and also private data of individuals, including their demographic, geographic and other identification features such as Name, age, gender, address, AADHAR number etc., including the data of AP Smart Pulse Survey data of State Resident Data Hub (SRDH) data of Praja Sadhikara Vedika (managed) by Karvy Data Management Services Ltd., Hyd), data of IVRS surveys conducted by Govt of AP. All the above data is used by M/s.IT GRIDS (India) Pvt Ltd, Hyderabad in the mobile app developed in the name of Savamitra in violation of Hon'ble Supreme Court orders issued in W.P. (Civil) No. 494 of 2012 (Justice K.S.Puttaswamy and Union of India & Others). Further no request was made by any political party for color photographs of voters nor does the ECI have any record of having provided such data to any political party or individual for using it officially. Through illegally acquired data, without consent of individuals the above agencies have been making the identification, demographic, geographic, socio-economic data available to unauthorized people who are using Sevamitra application. The availability of such information in public domain poses great risk to each and every voter in Andhra Pradesh. They are also making use of this data to analyze who are for and who are against to the ruling government and based on this analysis, they have deleted from the Electoral Rolls. These voters are existing in the 2014 electoral rolls but now, their votes have disappeared in 2019 electoral rolls. The names of such votes for ex are Sreedhar Reddy Nalivela (ID No.RTT0112169), EmManikanta (ID No. IAX0108092), Dadigelabavaiah (ID No.RRV0626184) and Anuradha (ID No.AYM0262691).Hence requested to take action against the management of M/s. IT Grids (India) Pvt. Ltd, PLOT - 538, 5<sup>th</sup> Floor, Krishna Heights, Ayyappa Society, KHANAMET, MADHAPUR, SERILINGAMPALLY, Hyderabad, Telangana for committing offences U/s. 120 (B), 379, 420, 188 IPC and Section 66 (B) and 72 of Information Technology Act. Hence FIR.

Received on 02.03.2019 at 0015 hours.

112

As per the contents of the above petition, I registered a case in Cr.No. 174/2019, U/Sec. 120 (B), 379, 420, 168 IPC and Section, 66(B) and 72 of Information Technology Act and took up the investigation.

13. Action taken.

Since the above information reveals commission of offence (s) u/s as mentioned at item NO.2:

(1) Registered the case and took up the investigation or : Name: Y  
Nageswar Rao

(2) Directed to take up the Investigation or Rank: Inspector

(3) Refused investigation due to.....

(4) Transferred to P.S.....District.....on point of  
jurisdiction

F.I.R. read over to the complainant/informant, admitted to be correctly recorded and a copy give to the complainant/informant, free of cost.

Signature of Officer In-charge, Police Station

14. Signature/Thumb Impression  
of the complainant/informant

Name Y Nageswar Rao  
Rank Inspector

15. Date & Time of Dispatch to the Court : 02/03/2019 00:20

///TRUE COPY//

113

ANNEXURE P- II



भारतीय रिज़र्व बैंक  
RESERVE BANK OF INDIA  
www.rbi.org.in

RBI/2010-11/389

DBOD.AML.No. 77 /14.01.001/2010-11

January 27, 2011

The Chairmen / CEOs of all Scheduled Commercial Banks (Excluding RRBs)/  
Local Area Banks / All India Financial Institutions

Dear Sir,

Opening of "Small Account"

Please find enclosed a copy of the Government of India, Notification No. 14/2010/  
F.No.6/2/2007-E.S. dated December 16, 2010, amending the Prevention of Money-  
laundering (Maintenance of Records of the Nature and Value of Transactions, the  
Procedure and Manner of Maintaining and Time for Furnishing Information and  
Verification and Maintenance of Records of the Identity of the Clients of the Banking  
Companies, Financial Institutions and Intermediaries) Rules, 2005.

**A. Small Accounts**

2. In terms of Rule 2 clause (fb) of the Notification 'small account' means a savings  
account in a banking company where-

- (i) the aggregate of all credits in a financial year does not exceed rupees one lakh;
- (ii) the aggregate of all withdrawals and transfers in a month does not exceed  
rupees ten thousand; and
- (iii) the balance at any point of time does not exceed rupees fifty thousand .

3. Rule (2A) of the Notification lays down the detailed procedure for opening 'small  
accounts'. Banks are advised to ensure adherence to the procedure provided in the  
Rules for opening of small accounts.

Department of Banking Operations and Development, Central Office, C.O. Building, 13th Floor, Fort,  
Mumbai, 400001

टेलिफोन /Tel No.:022-22601000 फैक्स/Fax No.:022-22701239 Email ID:cgmicdbodco@rbi.org.in

हिंदी उपसंहार है, प्रत्यक्ष प्रयोग बहारा

114



**B. Officially Valid Documents**

4. The Notification has also expanded the definition of 'officially valid document' as contained in clause (d) of Rule 2(1) of the PML Rules to include job card issued by NREGA duly signed by an officer of the State Government or the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

5. It is further advised that where a bank has relied exclusively on any of these two documents, viz. NREGA job card or Aadhaar letter, as complete KYC document for opening of an account (ref. paragraph 2.4 (f) of the Master circular dated July 1, 2010) the bank account so opened will also be subjected to all conditions and limitations prescribed for small account in the Notification.

6. Accordingly, all accounts opened in terms of procedure prescribed in Rule 2A of the Notification enclosed and all other accounts opened ONLY on the basis of NREGA card or Aadhaar letter should be treated as "small accounts" subject to the conditions stipulated in clause (i) to (v) of the sub-rule (2A) of Rule 9.

7. Please acknowledge receipt.

Yours faithfully,

(Vinay Baijal)  
Chief General Manager

Encl: As above

115

Government of India  
Ministry of Finance  
(Department of Revenue)

Notification

New Delhi, the 16<sup>th</sup> December, 2010

GSR (E) – In exercise of the powers conferred by sub-section (1) read with clauses (h) (i), (j) and (k) of sub-section (2) of Section 73 of the Prevention of Money-laundering Act, 2002 (15 of 2003), the Central Government hereby makes the following amendments to the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, namely:-

1. (1) These rules may be called the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Third Amendment Rules, 2010.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. In the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, -

(a) in rule 2,-

(i) after clause (b), the following clause shall be inserted, namely:-

“(bb) “Designated Officer” means any officer or a class of officers authorized by a banking company, either by name or by designation, for the purpose of opening small accounts”.

(ii) in clause (d), for the words “the Election Commission of India or any other document as may be required by the banking company or financial institution or intermediary”, the words “Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the Reserve Bank of India or any other document as may be required by the banking companies, or financial institution or intermediary” shall be substituted;

(iii) after clause (fa), the following clause shall be inserted, namely:-

“(fb) “small account” means a savings account in a banking company where-

116

- (i) the aggregate of all credits in a financial year does not exceed rupees one lakh,
- (ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand, and;
- (iii) the balance at any point of time does not exceed rupees fifty thousand”.

(b) In rule 9, after sub-rule (2), the following sub-rule shall be inserted, namely:-

“(2A) Notwithstanding anything contained in sub-rule (2), an individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account.

Provided that –

(i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;

(ii) a small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;

(iii) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months.

(iv) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through the production of officially valid documents, as referred to in sub rule ( 2) of rule 9”; and

(v) foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established through the production of officially valid documents, as referred to in sub-rule (2) of rule 9.”

(Notification No.14/2010/F.No.6/2/2007-ES)

(S.R. Meena)  
Under Secretary

Note: The principal rules were published in Gazette of India, Extraordinary, Part-II, Section 3, Sib-Section (i) vide number G.S.R.444 (E), dated the 1<sup>st</sup> July, 2005 and subsequently amended by number G.S.R.717 (E), dated the 13<sup>th</sup> December, 2005, number G.S.R. 389(E), dated the 24<sup>th</sup> May, 2007, number G.S.R. 816(E), dated the 12<sup>th</sup> November, 2009, number G.S.R.76 (E), dated the 12<sup>th</sup> February, 2010 and number G.S.R. 508(E), dated the 16<sup>th</sup> June, 2010.

117

ANNEXURE P-12



भारतीय रिज़र्व बैंक  
RESERVE BANK OF INDIA  
www.rbi.org.in

RBI/2011-12/207

DBOD.AML.BC.No. 36/ 14.01.001/2011-12

September 28, 2011

The Chairmen/CEOs of all Scheduled Commercial Banks (Excluding RRBs)/  
Local Area Banks/All India Financial Institutions

Dear Sir,

Know Your Customer Norms – Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number

Please refer to the Government of India Notification No. 14/2010/F.No. 6/2/2007-ES dated December 16, 2010 which recognises the letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number, as an officially valid document as contained in Rule 2(1)(d) of the PML Rules, 2005.

2. In this regard, a reference is invited to paragraph 5 of our circular DBOD.AML.No.BC.77/14.01.001/2010-11 dated January 27, 2011, wherein it was stipulated that when bank relies exclusively on the Aadhaar letter as complete KYC document for opening of an account, such an account would be subject to all conditions and limitations applicable to 'Small' accounts as detailed in the Govt notification referred to above. After further consultations with Government, it has now been decided to accept the letter issued by the UIDAI as described above as an officially valid document for opening bank accounts without the limitations applicable to 'Small' accounts as prescribed in paragraph 5 of our circular under reference.

3. In this connection, attention is also invited to paragraph 2.4 (f) of the Master Circular on KYC/AML/CFT dated July 01, 2011, dealing with customer identification. It is reiterated that while opening accounts based on Aadhaar also, banks must satisfy themselves about the current address of the customer by obtaining required proof of the same as per extant instructions.

4. Please acknowledge receipt.

Yours faithfully,

(Deepak Singhal)  
Chief General Manager in-Charge

118

Government of India  
Ministry of Finance  
(Department of Revenue)

Notification

New Delhi, the 16<sup>th</sup> December, 2010

GSR (E) – In exercise of the powers conferred by sub-section (1) read with clauses (h) (i), (j) and (k) of sub-section (2) of Section 73 of the Prevention of Money-laundering Act, 2002 (15 of 2003), the Central Government hereby makes the following amendments to the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, namely:-

1. (1) These rules may be called the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Third Amendment Rules, 2010.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. In the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, -

(a) in rule 2,-

(i) after clause (b), the following clause shall be inserted, namely:-

“(bb) “Designated Officer” means any officer or a class of officers authorized by a banking company, either by name or by designation, for the purpose of opening small accounts”.

(ii) in clause (d), for the words “the Election Commission of India or any other document as may be required by the banking company or financial institution or intermediary”, the words “Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the Reserve Bank of India or any other document as may be required by the banking companies, or financial institution or intermediary” shall be substituted;

(iii) after clause (fa), the following clause shall be inserted, namely:-

“(fb) “small account” means a savings account in a banking company where-

119

- (i) the aggregate of all credits in a financial year does not exceed rupees one lakh,
- (ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand, and;
- (iii) the balance at any point of time does not exceed rupees fifty thousand”.

(b) In rule 9, after sub-rule (2), the following sub-rule shall be inserted, namely:-

“(2A) Notwithstanding anything contained in sub-rule (2), an individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account.

Provided that –

- (i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;
- (ii) a small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;
- (iii) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months.
- (iv) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high-risk scenarios, the identity of client shall be established through the production of officially valid documents, as referred to in sub rule ( 2) of rule 9”; and
- (v) foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established through the production of officially valid documents, as referred to in sub-rule (2) of rule 9.”

(Notification No.14/2010/F.No.6/2/2007-ES)

(S.R. Meena)  
Under Secretary

Note: The principal rules were published in Gazette of India, Extraordinary, Part-II, Section 3, Sib-Section (i) vide number G.S.R.444 (E), dated the 1<sup>st</sup> July, 2005 and subsequently amended by number G.S.R.717 (E), dated the 13<sup>th</sup> December, 2005, number G.S.R. 389(E), dated the 24<sup>th</sup> May, 2007, number G.S.R. 816(E), dated the 12<sup>th</sup> November, 2009, number G.S.R.76 (E), dated the 12<sup>th</sup> February, 2010 and number G.S.R. 508(E), dated the 16<sup>th</sup> June, 2010.

Printed from  
THE TIMES OF INDIA

# SBI alleges Aadhaar data misuse, UIDAI rubbishes charge

TNN | Jan 29, 2019, 02:39 AM IST



CHANDIGARH/JIND: Officials of State Bank of India (SBI) have alleged that data of the Unique Identification Authority of India (UIDAI) has been misused. Logins and biometrics of their Aadhaar operators have been misused to generate unauthorised Aadhaar cards, bank officials informed UIDAI. Countering the charge, UIDAI said, "Aadhaar database is fully secured and no security breach, biometric or otherwise, has taken place."

SBI, like other banks, was given an Aadhaar enrolment target for which it selected vendors — FIA Technology Services Pvt Ltd and Sanjivini Consultants Pvt Ltd — in the Chandigarh region which covers Haryana, Punjab, Himachal, J&K and the UT of Chandigarh itself. However, of close to 250 operators employed with these agencies, nearly half were

*SBI alleges Aadhaar data misuse, UIDAI rubbishes charge*  
penalised in the last two months and were either deactivated or blacklisted. This brought SBI's Aadhaar enrolments to a halt at many branches, causing the bank to fail to meet targets and face penalties.

## CONFLICTING CLAIMS

▶ SBI given Aadhaar

121

➤ SBI gives UIDAI enrolment target for which it selected vendors in Chandigarh. Of 250 operators employed with these agencies, **half were penalised**

➤ UIDAI says an operator, Vikram, used his ID to **generate Aadhaar cards using fraudulent documents.**

It was done using 'multiple station IDs' in his name

➤ SBI officials say only they could have approved multiple

station IDs but they had not.  
Claim there **must have been lacunae in UIDAI system**

➤ **UIDAI** says Aadhaar database **fully secured** and no breach has taken place

122

One of those penalised was 40-year-old Vikram, who worked for a monthly salary of Rs 10,000 as an Aadhaar operator at the SBI branch in a small village called Uchana in Haryana's Jind district. On December 26, 2018, UIDAI fined him more than Rs 33 lakh.

According to UIDAI, Vikram had used his operator ID to generate Aadhaar cards using fraudulent documents between November 9 and November 17, 2018. It was done using "multiple station IDs" in Vikram's name, which allowed Aadhaar cards to be made from multiple devices — 143, to be precise. Every device, like a laptop, desktop or tablet, used for Aadhaar enrolment is registered with UIDAI and identified by the "station ID".

SBI officials pointed out that as "registrar" (as all banks entrusted with Aadhaar enrolment are), only they could have approved multiple station IDs but they had not done so. The bank's officials in Chandigarh wrote to their corporate office in Mumbai to

20/03/2019

SBI alleges Aadhaar data misuse, UIDAI rubbishes charge - Times of India

✓✓

raise the issue with UIDAI, saying they did not create these multiple station IDs and there must have been lacunae in UIDAI's security system that allowed "someone to hack the system and generate multiple station IDs" in Vikram's name.

Even more baffling was the misuse of Vikram's personal biometrics (fingerprints in this case) to generate Aadhaar cards, carry out unexplained transactions at places like the I-T department, Maharashtra government, MP government, National Informatics Centre and various banks, and even withdraw money from his personal accounts. All this time, UIDAI did not act against any bank official, which would have been the case had there been a lapse or wrongdoing by SBI officials.



ALSO READ

[UIDAI dismisses reports on Aadhaar software hacking](#)

SBI deputy general manager B Rajendra Kumar confirmed that he was aware of the "misuse of the biometrics" of Vikram and problems facing their sub-vendors. "We have, through our corporate office in Mumbai, raised this issue with UIDAI. The authority should be more transparent with us and let us know how this is happening. They should also guide us on the issue and, above all, make their database more secure," he told TOI.

An internal inquiry by the bank, and also the agency (vendor), cleared Vikram of the charges levelled by UIDAI, and SBI has already requested the authority to remove the penalty and allow him to return to work. Seeking UIDAI's response, TOI wrote a mail to its chief executive officer (CEO) and media in-charge on January 4, 2019. In its reply, sent January 18, UIDAI refused to share the details of the case but admitted that an inquiry was on.



ALSO READ

[Airtel, Axis Bank fined for UIDAI term breach](#)

124

Meanwhile, almost all the operators, except Vikram, were cleared by UIDAI and allowed to return to work. On January 9, the authority finally introduced an additional step in the registration of Aadhaar operators as an extra security measure.

"Also, some unscrupulous elements have been attempting to register multiple machines but UIDAI has an inherent system in place to detect any such attempt and appropriate action is taken on a daily basis on operators who err. UIDAI imposes financial disincentives and blacklists errant operators. However, it relooks into the issue if someone is wrongly penalised. It would be pertinent to mention here that divulging details of any specific case under inquiry would not be appropriate in the interest of the case," UIDAI told TOI when specifically asked about Vikram's case.

[Read this story in Bengali](#)

[Read this story in Marathi](#)

BAR &  
BENCH

125

ANNEXURE P- 14

20/03/2019

Scroll - Aadhaar details of enrolment operator stolen and misused show UIDAI records: Report

Scroll.in

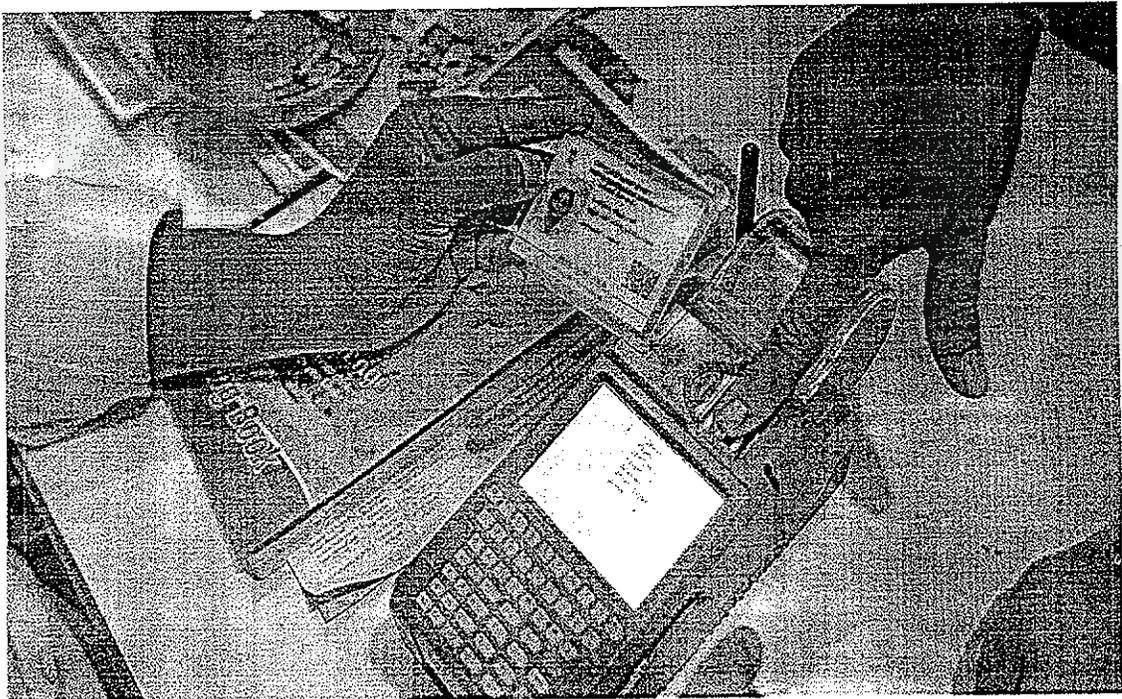
AADHAAR CONTROVERSY

## Aadhaar details of enrolment operator stolen and misused, show UIDAI records: Report

In November 2018, the UIDAI had barred Vikram Sheokhand after his credentials were used in multiple cities in a single day.

by Scroll Staff

Published Feb 20, 2019 · 05:34 pm



Representative Image. | Noah Seelam/AFP

The biometric details of an Aadhaar operator in Haryana's Jind was allegedly stolen and misused, with the credentials being used in multiple cities in a single day, *Huffpost India* reported on Wednesday. The Unique Identification Authority of India had barred Vikram Sheokhand in November 2018 from working as an Aadhaar enrolment operator for five years, after they detected that his credentials were being misused.

Going by the UIDAI's records, Sheokhand's digital fingerprints were used on November 12, 2018, at three bank branches in Haryana, and the Madhya Pradesh State Electronics Development Corporation in Bhopal - each transaction was a few hours apart. However, Sheokhand insisted that he was in Uchana village of Jind, where he works as the Aadhaar operator at the State Bank of India office, at that time.

126

20/03/2019

Scroll - Aadhaar details of enrolment operator stolen and misused show UIDAI records: Report

"I am not a ghost who can travel from Jind to Madhya Pradesh in less than a second and simultaneously work in SBI's branch in Uchana," Sheokhand told *HuffPost India*.

Sheokhand is one of several Aadhaar operators who were penalised last year after their login and biometric details were misused to generate unauthorised Aadhaar cards. FIA Technology Services Private Limited and Sanjivini Consultants Private Limited were assigned as vendors to SBI in Chandigarh region to reach its Aadhaar enrolment target. The Chandigarh region includes Haryana, Punjab, Himachal Pradesh, and Jammu and Kashmir, besides the Union Territory of Chandigarh itself.

However, nearly half of the Aadhaar operators associated with these agencies were penalised, and were either deactivated or blacklisted. Sheokhand has been penalised Rs 33 lakh for alleged fraudulent transactions. His employer FIA Technology Systems said the UIDAI is investigating the case.

### Digital fingerprints possibly still at large

The UIDAI has asked Sheokhand to lock his biometrics that would temporarily disable his Aadhaar authentication. However, he continues to receive automated email alerts informing him that someone had tried to log into the Aadhaar system using his fingerprints, but had failed since his details are locked, *Huffpost India* reported. This suggests that the digital copies of his fingerprints are still at large.

"What if someone misuses my biometrics and frames me in some major financial fraud, or plans some major terror activity?" Sheokhand told the news website. "I am terrified every time I unlock my biometrics on the UIDAI server."

Since the UIDAI blacklisted him, Sheokhand has been working as a computer operator in a rural citizen service centre, helping citizens access various schemes. However, this too requires him to use biometrics in order to access specific government portals.

It is unclear where the UIDAI has lifted Sheokhand's fine.

---

© 2019 Scroll.in

IN THE SUPREME COURT OF INDIA  
CIVIL ORIGINAL JURISDICTION  
W.P.(C) \_\_\_\_\_ OF 2019

**IN THE MATTER OF:**

S.G. VOMBATKERE & ANR

...PETITIONERS

Versus

UNION OF INDIA & ANR.

...RESPONDENTS

**APPLICATION FOR STAY**

**MOST RESPECTFULLY SHOWETH:**

1. That the captioned Writ Petition under Article 32 of the Constitution of India has been filed in public interest challenging the constitutional vires of the Aadhaar & Other Laws (Amendment) Ordinance 2019 (hereinafter, "impugned Ordinance") and the Pricing of Aadhaar Authentication Services Regulations, 2019 (hereinafter, "impugned Regulations"), on the grounds *inter alia* that they violate the fundamental rights guaranteed under Part III of the Constitution of India.
2. That the Petitioners are citizens of India and are public-spirited citizens, who have approached this Hon'ble Court for the protection of the fundamental rights of the citizens of India.
3. That the contents of the captioned Writ Petition are not repeated herein for the sake of brevity, but may be read as part and parcel of this Application.

4. That in light of the facts mentioned in the Writ Petition and hereinabove and the submissions made, the triple test of *prima facie* case, balance of convenience in favour of the Applicant; and grave and irreparable loss and damage is satisfied in the instant case.

5. *Prima facie case.*

(i) The submissions and the grounds in the Petition demonstrate manifest unconstitutionality of the Impugned Ordinance and the Impugned Regulations. *Inter alia*, they seek to re-legislate the provisions of the Aadhaar Act that enabled, whether intended or otherwise, commercial exploitation of personal information collected for the legitimate purposes of the State. Such provisions and enablement of commercial exploitation had been specifically declared unconstitutional vide the Constitution Bench judgment in *Justice (Retd). K.S. Puttaswamy v. Union of India* [(2019) 1 SCC 1]. It is therefore prayed for herein that a stay of the Impugned Ordinance and the Impugned Regulations is not only warranted but necessary to uphold the Rule of Law and to give effect to the judgment of this Hon'ble Court.

(ii) Furthermore, due to the deeply flawed enrollment system to create the Aadhaar database, the information available with the 2nd Respondent is unverified by any government agency and lacks integrity. The purported utilization of the same for verification of identity for the use of services under the Prevention of Money Laundering Act, 2002 and the Indian Telegraph Act, 1885 is

manifestly arbitrary, and compromises national security and the integrity of the financial system of the country.

- (iii) Without prejudice to (i) and (ii) above, it is also stated herein that the principles of law governing grant of stay against Acts of Parliament or State Legislatures do not apply to Ordinances, but instead only the principles that govern the stay of executive actions apply to Ordinances, which are effectively only executive *fiats* that are yet to receive the approval of the legislature.

*6. Irreparable Injury & Balance of Convenience*

The submissions and the grounds in the Petition demonstrate a manifest infringement and violation of fundamental rights of Indian citizens, including the violation of their fundamental right to privacy, as a result of the operation of the impugned Ordinance and the impugned Regulations. As such injury is caused to public at large and is not reparable or justifiable at a personal level, a stay of the operation of the impugned Ordinance and the impugned Regulations is necessary and warranted.

7. That the present Application has been moved bona-fide and may be allowed in the interests of justice.

**PRAYER**

In light of the submissions and averments above, this Hon'ble Court be pleased to

- a) Pass an Order staying the operation of the Aadhaar & Other Laws (Amendment) Ordinance, 2019; and

- b) Pass an Order staying the operation of the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019; and
- c) Pass any further order or direction in the interests of justice and in the facts and circumstances of this case.

FOR WHICH ACT OF KINDNESS, THE APPLICANTS SHALL AS IN DUTY BOUND, EVER PRAY.

**DRAWN BY:**  
PRASANNA S.  
ADVOCATE

**FILED BY:**



**VIPIN NAIR**  
ADVOCATE-ON-RECORD  
FOR THE PETITIONERS

DRAWN ON:-04.4.2019  
FILED ON:-16.04.2019  
NEW DELHI