IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. _____ OF 2019

(UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA)

BETWEEN

...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 3RD 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) Act, 2019 as ultra vires, unconstitutional, null and void and in particular violative of Articles 14, 19 and 21 of the Constitution of India."

. 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 Petitioner has already filed his income tax returns for the year 2019-20, and all previous years. However due to privacy concerns which would arise from revealing these details in open court,

ANNEXURE P-1 at page .

1(b). The 2nd petitioner is a citizen of India and is also engaged

he is also actively involved in a public interest litigation pending before

The subject matter of that petition is strict implementation of the

. 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 Petitioner has already filed his income tax returns for the year 2019-20, and all previous years. However due to privacy concerns which would arise from revealing these details in open court, Petitioner

P-2 at pages _____.

The Petitioners are providing their personal details to fulfil the requirements prescribed under the Supreme Court Rules, under protest, since they are concerned with the privacy implications of disclosing such details publicly.

1(c). The petitioners herein filed Civil Writ Petition No. 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 challenging the

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. The final judgment and order in Writ Petition of

1(d). The Petitioners have filed a review petition bearing No._____ 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. The Petitioners have also filed

Notice was issued on this on 5th July 2019.

1(e). Due to Section 139AA of the Income Tax Act, 1961, which mandates Aadhaar linkage with an income tax payer's PAN, Petitioner No.1 was constrained to obtain an Aadhaar number because he was unable to file his IT Return for A.Y 2019-20 without quoting Aadhaar number, in spite of attempts at manual filing of his IT Return. His Aadhaar number was generated on 25.7.2019. Petitioner No.2 does not have an Aadhaar number.

The Respondents

2(a). The 1st Respondent is the Union of India.

2(b). The 2nd 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 challengethe Aadhaar and Other Laws Amendment Act, 2019 ("**impugned Act**") 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 Act 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 2nd 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 Act, 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 Actwill result in the creation of a surveillance state and the Aadhaar database will be exploited by private players for commercial gain. Moreover, the impugned Act 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 Act 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 Act, 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 hence filed a review petition.

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 authenticatingon every occasion that they

authenticate their biometrics. Coupled with the extensive mandatory use of Aadhaar which was being compelled on all citizens (which continues to be compelled on citizens in certain areas) 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 violations caused by the Aadhaar project.

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 Act, 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. In fact, the attached graph showing usage of Aadhaar for e-KYC, taken from the UIDAI website in July 2019, shows how the number of Authentication requests fell right after the judgment, but rose around the Aadhaar and Other Laws (Amendment) Ordinance, 2019was promulgated, in March 2019. This increase in number of users is precisely what the Supreme Court was trying to contain vide its judgement, and permitting this to increase, as will be the inevitable outcome of the impugned Act, goes against this. The chart showing e-KYC usage from September 2018 to July 2019 is annexed herewith as **ANNEXURE P-3 from pages __ to __.**

17. 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 Act, 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.

18. 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 Act 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

19. This petition challenges the Aadhaar and Other Laws (Amendment)Act, 2019inasmuch as it violates and threatens to violate the fundamental rights of the Petitioners and other citizens of India. The impugned Act, 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".

20. The Petitioners seek appropriate declarations to the effect that the impugned Act is *ultra vires* the Constitution of India. Should this Court uphold the validity of the impugned Act, the petitioners urge an alternative case that key portions of the impugned Act are *ultra vires* the Constitution of India and seek appropriate declarations with respect to the unconstitutionality of those particular provisions.

21. The impugned Act was published in the Gazette of India on 24th July 2019, and was notified on 25th July 2019. A copy of The Aadhaar and other Laws (Amendment) Act, 2019, No. 14 of 2019 as published in the Gazette of India on

24th July 2019, was notified on 25th July 2019 is annexed and marked as **ANNEXURE P-4 at pages __ to __**.

22. 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 Regulations were published in the Gazette of India on 6th March 2019. A copy of the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 is annexed and marked as **ANNEXURE P-5 at pages** __ to _____.

23. The petitioners are also challenging Section 2(3) Aadhaar (Pricing of Authentication Services) Regulations 2019, demonstrates that the government is exercising coercion on enrolment registrars to increase the number of enrolments, by setting enrolment targets and levying charges on entities not achieving those targets. The Section states:

> "2 (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-+th 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."

E. BRIEF FACTS

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. The Aadhaar and Other Laws (Amendment) Bill, 2019 ("**Aadhaar Amendment Bill, 2019**) was passed in Lok Sabha on 04.01.2019, after one day of debate. It was described as a Bill to amend the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefitsand Services) Act, 2016 and further to amend the Indian TelegraphAct, 1885 and the Prevention of Money-laundering Act, 2002It was then pending before the Rajya Sabha, when the Lok Sabha dissolved.

32. The Aadhaar Amendment Bill, 2019 lapsed.

33. The Aadhaar and Other Laws (Amendment) Ordinance, 2019 was promulgated by the President of India on 2nd March 2019. This was identical to the Aadhaar Amendment Bill, 2019, which had lapsed.

34. 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.

35. The Petitioners herein filed W.P. (Civil) No.679 of 2019, challenging the impugned Ordinance. Notice was issued on this petition on 5.07.2019.

36. The Aadhaar and Other Laws (Amendment) Bill, 2019, was passed by the Lok Sabha on 4th July 2019. It was passed by the Rajya Sabha on 8th July 2019, and was published in the Gazette on 24thJuly, 2019. It was notified on 25th July 2019.

F. LACK OF INTEGRITY IN AADHAAR DATABASE

37. The Petitioners state that the database of demographic and biometric information collected and stored by the 2nd Respondent lacks integrity.

38. 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.

39. The data stored with the 2nd 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.

40. The 2nd 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.

41. The 2nd 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.

42. 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

43. 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 numberagainst 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 automatically 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, the Aadhaar system 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 wired and 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. his is precisely the invaluable metadata which is used by security

and commercial intelligence agencies for untargetted (mass) surveillance, and/or profiling for security or commercial purposes.

44. 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 Act. 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.

45. 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 Act. 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.

46. The upshot is that if the impugned Act 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 which was re-verified for the purpose of the challenge to the Aadhaar and Other Laws (Amendment) Ordinance, 2019, 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-6 at pages to .**

(ii) Jude Terrence D'Souza in an affidavit dated 22.11.2016 filed on behalf of the petitioners in the Aadhaar case (and which was re-verified for the purpose of the challenge to the Aadhaar and Other Laws (Amendment) Ordinance, 2019, by an affidavit dated11.04.2019) 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-7 at pages to .**

47. 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-8 at pages to .**

48. 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 Act enables and the impugned Regulations incentivise.

H. GROUNDS TO CHALLENGE THE AADHAAR AND OTHER LAWS (AMENDMENT) ACT, 2019

49. The Petitioners submit that the Aadhaar and Other Laws (Amendment) Act, 2019 (No. 14 of 2019) ("**impugned Act**") 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 Act is unconstitutional as it violates the rights guaranteed under Part III of the Constitution. It enables State surveillance and private surveillance of citizens, andcommercial 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 demographicinformation 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 disbursal 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 Act goes against this unequivocal restriction by opening up the Aadhaar system to private entities. This is constitutionally impermissible.

Sections 6, 26 and 27 of the impugned Act effectivelyrestore 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 Act.

(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-9 pages to .**

- Newspaper articles entitled (ii) "TDP app breached data of 3.7cr voters? Probe begins," Times News Network dated 26.02.2019 **P-10 at pages to .**
- 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-11 at pages to**

(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 (ii) used for commercial profiling.

- **Surveillance architecture**

(g) By permitting private entities to join the Aadhaar ecosystem, the impugned Act exacerbates the threat ofsurveillance 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) In the Privacy Judgement, the Supreme Court 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)

(j) In the Aadhaar judgement, Justice Chandrachud 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 integrityand has no value other than, at most, the underlying documents on the basis of which the Aadhaar numbersare 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 26and 27of the impugned Actwhich seeks to amend the Indian Telegraph Act, 1885 and Prevention of Money Laundering Act, 2002 respectively, suffer from over-inclusiveness and are 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-12 at pages to and P-13 at pages to** .

(f) Furthermore, the efficacy of Aadhaar is dependent on other Proof of Identity and Proof of Address documentsand not on independent verification of identity. This is outlined in the UIDAI's Demographic Data Standards and Verification Procedure ("**DDSVP**") 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 *DebashisNandy 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-14 at pages to and ANNEXURE P-15 at pages to** .

(i) In view of the lack of sanctity of the Aadhaar database, Sections 26 and 27 of the impugned Act, which amend Section 4 of the Indian Telegraph Act, 1885, and the Prevention of Money Laundering Act, 2002,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 Actpermits 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 Act which facilitates the same is unconstitutional for this ground alone.

C. Section 9, read with Section 3(v), of the impugned Act,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. How this is to be done is not defined in the Aadhaar Act or the impugned Act.

As per the UIDAI's website, offline verification is presumably 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. A description of the use of XML files is annexed as **ANNEXURE P-16__ from pages __ to __**.

However, 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 Actintroduces 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 Act,sets out certain conditions under which offline verification may be carried out. The provision states that offline verificationcan 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, 2002and periodic circulars and guidelines issued by theRBI. The impugned Act 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 Act 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, as introduced by Section 6 of the impugned Act.

(a) Under the newSection 4(7) of the Aadhaar Act as introduced by the impugned Act, the Parliament can make Aadhaar authentication mandatory for any purpose. The impugned Act

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 Act 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 Act, in Section 14, amends Section 33(2) of the Aadhaar Act. This provision 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 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 12 of the impugned Act 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.

H. Section 7 of the impugned Act, amends Section 7 of the Aadhaar Act and increases the ambit of Aadhaar to cover the Consolidated Fund of the State. This is an impermissible expansion as it violates the federal structure of India. In addition, this increases the risk of surveillance and poses an impermissible threat to privacy, through the creation of federated databases which will contain persons' Aadhaar number, and biometric and demographic details.

I. Under the federal structure of India, a central law cannot regulate the process by which States decide to disburse funds from the Consolidated Fund of States. The Consolidated Fund of the State is defined under Article 266 of the Constitution of India, as distinct from the Consolidated Fund of India. It is under the power of the State government, and can only be disbursed in the manner provided for under the Constitution. This manner is further explained in Article 283 (2), a provision dealing with the custody of the Consolidated Fund of States. Under this provision, custody of the Consolidated Fund of the State, and "all other matters connected with or ancillary to matters aforesaid shall be regulated by law made by the Legislature of the State." This

would include the manner in which States choose to disburse these funds. The Union cannot assume control over this aspect of the procedure for disbursal of fund from the Consolidated Fund of States.

J. As noted by this Hon'ble Court in S. R. Bommai v. Union of India (1994 3 SCC 1), federalism is part of the basic structure of our constitution. Although the Constitution provides more power to the centre, within their sphere, states are supreme. As per Justice Sawant and Justice Kuldip Singh in S. R. Bommai v. Union of India (1994 3 SCC 1):

> 98. " …notwithstanding the fact that there are many provisions in the Constitution whereunder the Centre has been given powers to override the States, our Constitution is a federal Constitution. It means that the States are sovereign in the field which is left to them. They have a plenary authority to make any law for the peace, order and good Government of the State.
>
> (Paragraph 98)
>
> 99. The above discussion thus shows that the States have an independent constitutional existence and they have as important a role to play in the political, social, educational and cultural life of the people as the Union. They are neither satellites nor agents of the Centre…"
> [Paragraph 99]

(a) In any event, the Centre has no legislative or executive power to regulate matters which are covered under List II of Schedule VIII, including welfare schemes which the States operate. It is impermissible, within our Constitutional scheme, for the Union government to assume control over how these schemes are to be implemented, including the process of identifying beneficiaries.

(b) Permitting states to access the Aadhaar database, will also lead to the creation of federated databases, which cause a threat to privacy. This was specifically addressed by the Hon'ble Supreme Court during the course of the hearing on the justiciability of Aadhaar. The Union of India has stated, by way of Counter Affidavit dated 09.03.2018 which was submitted in the Aadhaar matter W.P. (Civil) No. 829 of 2013, said that "registrar packets", which contained the demographic data of persons and were saved in State Resident Data Hubs, had been deleted. It also stated that Aadhaar did not enable or perpetuate "360-degree surveillance". However, enabling State governments to access this data through the introduction of Section 5A, re-opens the possibility of federated databases, and 360 degree surveillance by state governments.

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

50. 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. Theimpugned 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, Regulation 2(3) states,

> "Regulation 2(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 th 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."

This provision 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.

F. Section 2(3) of the Aadhaar (Pricing) Regulations 2019, clearly demonstrates that the government by arbitrarily setting enrolment targets and empowering itself to levy penalty charges on entities who can't achieve those targets, is exercising coercion on Aadhaar enrolment registrars and on persons who do not have Aadhaar. This is an impermissible exercise of power on the part of the State and in particular, the UIDAI.

J.JURISDICTION

51. 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 Act before this Hon'ble Court or any High Court. However, as set out above, the Petitioners have challenged the Aadhaar Ordinance in a previous petition, W.P. (Civil) No. 679 of 2019, which is materially the same as, and superseded by, the Aadhaar and Other Laws (Amendment)Act, 2019 challenged herein. This Hon'ble Court has issued notice in this petition by an order dated 05.07.2019. This order is annexed hereto and marked as **ANNEXURE P-17 at page __**.

K. PRAYERS

52. 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) Act, 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 Act ultra vires and unconstitutional:

(i) Section 6 of the impugned Act which introduces Section 4(7) to the Aadhaar Act.

(ii) Section 3 of the impugned Act which introduces Section 2(pa), 2(pb), and Section 9 of the impugned Act which introduces Section 8A to the Aadhaar Actand creates "offline verification".

(iii) Section 12 of the impugned Act which creates the "Unique Identification Authority of India Fund," under Section 25 of the Aadhaar Act.

(iv) Section 14 of the impugned Act, which amends Section 33(2) of the Aadhaar Act.

(v) Sections 26, and 25 of the impugned Act, which amend the Indian Telegraph Act, 1885 and the Prevention of Money Laundering Act, 2002.

d) This Hon'ble Court may be pleased to issue 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 certify 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

FILED BY:

ADVOCATE-ON-RECORD
FOR THE PETITIONERS

DRAWN ON:
FILED ON:-