IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. 1056 OF 2017

Nachiket Udupa & Another … PETITIONERS

VERSUS

Union of India & Others … RESPONDENTS

AND

WRIT PETITION (CIVIL) NO. 833 OF 2013

Aruna Roy & Another … PETITIONERS

VERSUS

Union of India & Others … RESPONDENTS

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

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

I. INTRODUCTION

A. PETITIONS BEFORE THIS HON'BLE COURT

1. W.P. (C) No. 1056/17 titled *Nachiket Udupa v UOI,* challenges the constitutional validity of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ["**Aadhaar Act**" or "**the Act**"] and the Regulations framed thereunder. It also challenges the directions dated 23.03.2017 issued by the Department of Telecom directing all Licensees to re-verify existing mobile subscribers through Aadhaar based e-KYC process ["**Impugned Direction**" **@pg 4-9, Vol. II**]. As an alternative, the Petitioners have also prayed for an option to "opt out" of the Aadhaar Project [**@pg 1-3, Vol I]**.

2. Petitioner No. 1 herein was compelled to obtain an Aadhaar number in order to register his marriage under the Special Marriage Act, 1954, and Petitioner No. 2 herein was required to enrol in Aadhaar in order to register the renewed lease agreement for his retail store.

3. W.P. (C) No. 833/13 titled *Aruna Roy v UOI* challenges the adoption of Unique Identification ["**UID**"] for the delivery of subsidies, benefits and services by the Central and State governments, *inter alia*, due to the widespread exclusion and denial of social welfare benefits, caused by the inherent design faults in the Aadhaar scheme.

B. CONSTITUTIONAL TESTS AND BREACHES

4. It is submitted that the constitutionality of the Aadhaar Act and the accompanying regulations must be examined on the touchstone of the test in ***Justice K.S. Puttaswamy (Retd.) v UOI*, (2017) 10 SCC 1, ¶¶ 310, 638** to assess whether the compulsion, and violation of privacy and personal liberty is just, fair, and reasonable on the following basis:

   a. Legality: which requires the existence of a valid law

   b. Legitimate State aim: which has to be judged at the highest standard of scrutiny (per ***Puttaswamy,* ¶¶ 378, 380** and ***V.G. Row*, AIR 1952 SC 196 @pg 72, Vol. I**), especially since the State cannot destroy human freedoms simply on the stated ground that it is building a welfare State (***Kesavanada Bharati v State of Kerala*, (1973) 4 SCC 225, ¶¶ 665-66 @pg 86, Vol. I**).

   c. Necessity and narrow tailoring: that the infringement must be *necessary* to achieve the stated aim, and must not infringe rights to an extent greater than that required to fulfil the aim. The corollary is that if there is an alternate way of achieving the aim, that *does not* involve infringement of rights, the impugned law is unconstitutional.

   d. Proportionality: that there must be a balance between the importance of the goal and the degree to which rights are infringed.

   e. Procedural safeguards: assessing whether there are safeguards in the Act that can ensure procedural due process.

5. It is submitted that the Aadhaar Act violates the fundamental rights of citizens, and falls foul of the **Puttaswamy** standard outlined above, in three different ways: at the point of *collection*, at the point of *storage*, and at the point of *use* (including authentication):

a. The architecture of the Act & associated notifications mandate the surrender of biometric data. The act of compulsion, at the stage of collection, lies in requiring individuals to part with such data, thus violating their rights to privacy and personal liberty. The State's justification for compulsion, viz. the targeted delivery of benefits, fails the due process and proportionality standard evolved under Art. 21 and ***Puttaswamy***, since it is based on preventive compulsion. Without having to show reasonable cause, the State requires an *entire population* to enrol in Aadhaar on the premise that *some* persons will be prevented from committing identity fraud. Such widespread presumption of criminality is as disproportionate, as it is unprecedented.

b. The centralised retention and storage of identity information in the Central Identities Data Repository ["**CIDR**"] is *per se* illegal and the prolonged retention of authentication requests/transaction logs is disproportionate. Further, the potential to interlink this data stored in various unrelated databases, through organic and inorganic seeding,[1] creates a chilling effect on personal autonomy and free exercise of individual liberties, apart from enabling a sophisticated surveillance infrastructure, which is violative of Art. 19 & 21.

c. The use of identity information by the State, without any purpose limitation or procedural safeguards, is disproportionate. The further use, under **sec. 7**, to require every resident to obtain Aadhaar and undergo authentication to avail guaranteed entitlements violates Art. 14 & 21. *First*, the denial of entitlements due to authentication failure (often due to age/ disability/manual labour) bears no rational nexus with the *eligibility* of individuals to receive entitlements. Thus, at the point of use, Aadhaar divides residents into two arbitrary classes: those who have Aadhaar (and those who do not) and those who can authenticate successfully (and those who cannot). *Secondly*, due to its automated, untested, and probabilistic[2] nature, Aadhaar has become a vehicle for exclusion, violating Art. 21's guarantee of right to life. *Finally*, the State has failed to discharge its burden of justifying the infringements since it has not demonstrated that Aadhaar is proportionate or the least restrictive way of achieving its stated goal [See **para 94-107 (*infra*)].**

C. ALL ACTS DONE PRIOR TO THE PASSAGE OF THE ACT ARE VOID *AB INITIO, AND ARE NOT SAVED/VALIDATED BY SEC. 59. IN ANY EVENT, SEC. 59 IS INVALID*

6. It is submitted that all acts done pursuant to the executive Notification dated 28.01.2009, under which the Aadhaar Program was created and implemented, violate fundamental

[1] Seeding is the process by which the Aadhaar number is introduced into various databases for identity verification. Inorganic seeding transpires when the database is automatically updated by the UIDAI using programming tools and algorithms, without the involvement of the Aadhaar number holder.

[2] See (a) **42nd Parliamentary Standing Committee @ pg 23, 32, 34, 35, 36, Vol. I)** and (b) **Report by UIDAI Committee on Biometrics on "Biometric Design Standards for UID Applications" (Dec 2009) @pg 44, 48, 56, Vol. I**

rights and are stillborn. It is also well settled that all executive action, which operate to the prejudice of any person, must have the authority of law to support it, and as a corollary, every act done by the government or its officers, must, if it is to operate to the prejudice of any person, be supported by some legislative authority [See ***Thakur Bharat Singh*, (1967) 2 SCR 454 @pg 290-92, Vol I]**. Further, a post-Constitutional law or executive act that violates fundamental rights is stillborn and void *ab initio* [See ***Deep Chand v State of UP* [1959] Supp. (2) SCR 8 @pg 143, 146-47, 163, Vol. I; *ML Jaini v State of UP* [1963] Supp. (1) SCR 912 @pg 210, 212-14, Vol. I;** and ***Rakesh Vij v Raminder Pal Singh Sethi (Dr.),* (2005) 8 SCC 504, ¶ 18 @pg 240-242 Vol. I].**

7. The State's failure to enact the Aadhaar Act for six years meant that all enrolments done between 2010-2016 were without any informed consent.[3] During this period, there were no statutory procedure that regulated the enrolment, storage, and further use of identity information [See ***S & Marper v UK*, (2008) ECHR 1581 (GC), ¶ 95 @pg 231, Vol. II**.] Consequently, the fundamental rights of citizens were being violated through the collection, storage, and use of their personal data by the State and private entities in a legislative vacuum, which was sought to be retrospectively validated by **sec. 59**.

8. It is well-settled that a validating law must remove the cause of invalidity of previous acts, and that a validating Act cannot be valid and effective if it simply deems a legal consequence without amending the law from which the said legal consequence could follow [See ***Delhi Cloth & General Mills Co. Ltd. v. State of Rajasthan*, (1996) 2 SCC 449, ¶12, 16-17** and ***Satchidananda Misra v. State of Orissa*, (2004) 8 SCC 599, ¶18-20**] The cause of invalidity in the present case was the *absence of a law* governing privacy infringements. Its cure must therefore be a legal fiction that deems the law to have always been in existence. However, **sec. 59** does not create such a legal fiction where the Aadhaar Act is deemed to have been in existence since 2009. It only declares a legal consequence of acts done by Union since 2009, which it cannot do.

9. Alternatively and without prejudice to the above, it is submitted that **sec. 59** is invalid and unconstitutional inasmuch as for Aadhaar enrolment done pre-2016, there was no informed consent or such other procedural guarantees and safeguards as are essential if the State seeks to infringe the right to privacy. Thus, even assuming (without conceding) that sec. 59 is a valid validating provision, at best, there would be a law, but none of the procedural guarantees or safeguards would in fact have been followed. Further, even the law would be invalid on the principle that legislative declarations of facts are not beyond judicial scrutiny. This Hon'ble Court can examine whether these so called facts were existent or non-existent and if the legislative declaration has been made by ignoring the facts in reality. In the present case, no procedural safeguards existed pre-2016 and thus, even

---

[3] See (a) ***CIWTC v. Brojo Nath Ganguly*, (1986) 3 SCC 156, ¶89 @pg 60 Vol. V** on an unfair or unreasonable contract; (b) ***Y.F. v Turkey*, (2003) ECHR 391, ¶ 34, 43 @pg 248, 250 Vol. II** and (c) ***Cruzan v Director, Missouri Dept. of Health*, 497 US 261 (1990) @ pg 397-398, Vol. III** on informed consent in a medical context.

assuming that sec. 59 is validly enacted, it has to be declared unconstitutional for violating Art. 14 and 21 [See ***Indra Sawhney v. UOI,*** **(2000) 1 SCC 168, ¶¶ 28-29, 36-40 @pgs 110, 115-116, Vol. I]**

II. COLLECTION OF IDENTITY INFORMATION UNDER THE AADHAAR ACT [SEC. 3, 4(3), 7 & ALLIED SECTIONS AND REGULATIONS] VIOLATES ART. 14 AND ART. 21

10. It is submitted that the commandeering by the State of the body of individuals, at the time of *collection,* by requiring them to present themselves to an enrolment centre to surrender their identity information, in order to be branded with a numerical identifier, violates the right to personal liberty. *First*, although framed as voluntary gateway for entitlements and services, Aadhaar is, in effect, mandatory. *Secondly*, the mandatory and compelled parting of identity information infringes the rights to privacy, bodily integrity, personal autonomy, and informational self-determination under Art. 21. *Thirdly*, this infringement necessitates heightened constitutional scrutiny in the context of the relationship between State and individuals (as opposed to between individuals and private corporations); and *fourthly*, this infringement is neither "just, fair, and reasonable" under Art. 21, nor is it proportionate.

A. THE AADHAAR ACT AND SURROUNDING INFRASTRUCTURE HAS MADE POSSESSION OF AADHAAR *DE FACTO* MANDATORY

11. Although the Aadhaar Act is ostensibly *framed* as a voluntary entitlement to establish one's identity [See **sec 3 r/w. 4(3)]**, the actions of the Executive and private entities under **secs. 7 & 57** have made possession of Aadhaar *de facto* mandatory. Residents have thus been forced to obtain an Aadhaar number, for continued access to statutory entitlements and services. Thus, at the stage of collection of identity information, there is compulsion:

a. 252 schemes have been notified by various Ministries/Departments of the Central Government under sec. 7 (as on 30.11.2017) requiring Aadhaar as a condition precedent for availing services, subsidies and benefits including for persons with disabilities, for SC/STs, and for rehabilitation of Manual Scavengers [**Reply to Lok Sabha Unstarred Qs No. 819 on 20.12.2017 @pg1-3, Vol II**. For the list of 139 notifications, see **pg 114-118, UOI's counter dated 30.10.2017 in WP No. 494/12]**

b. Aadhaar has been made mandatory for mobile phone services (**@ pg 4-9, Vol. II**); banking; tax payment; and online registration of students of CBSE-affiliated schools (**@ pg 10-11, Vol. II)**. It thus pervades every aspect of an individual's life.

12. Concomitantly, there is no **opt out** option in the Aadhaar Act, which makes consent irrevocable and deprives individuals the ability to make decisions about their life [See **Reply to Lok Sabha Unstarred Qs No. 2759 dated 03.01.2018 @ pg 12, Vol. II]**

13. In effect, the compulsion inherent in the Act denudes individuals of the right to decide how and in what manner to use their body and personal information. Sikri J. in ***NALSA v UOI,*** **(2014) 4 SCC 438, ¶¶ 91, 99, 104-108, @pg 69-74, Vol. II**, elaborated on the "right to

choice" being a fundamental principle that is inextricably linked with dignity and freedom of individuals, while the right not to be coerced was emphasised in ***Puttaswamy***.[4]

14. It is submitted that by introducing the element of *indirect* coercion, the operation of the Aadhaar Act, is one step short of forcing compliance through punishment, and two steps short of physically restraining individuals to obtain biometrics by force. If a citizen is shut out by the State from living a fulfilling life in society – unless biometrics are surrendered under the Act – it is merely achieving through indirect coercion, that which may be unseemly or illegal through physical coercion.

15. Pertinently, it is well settled that when the State makes the receipt of a benefit *conditional* upon an individual giving up or waiving constitutionally guaranteed rights, it is no longer a "voluntary" relationship between State and individual, but one that is marked by a potentially unconstitutional compulsion. Fundamental rights cannot be *bartered away* or *surrendered* by voluntary acts in return for aid. Marking out those who refuse to part with their data (by asserting their privacy) for deprivation of entitlements and services is an unconstitutional condition and an unreasonable classification, violative of Art. 14.

[See

(i) ***Ahmedabad St. Xavier's College Society v State of Gujarat,* (1974) 1 SCC 717, paras 158-171 @pg 120-122, Vol. II** that a condition may be invalidated because it penalises the exercise of a right by denying a benefit.

(ii) ***US v Butler*, 297 US 1 (1936) at 71, 74, @p 153-154, Vol. II** that the conditional form of power was unconstitutional because asserted power of choice was illusory

(iii) *TMA Pai v State of Karnataka,* (2002) 8 SCC 481, ¶ 312 @pg 344, Vol. VI

(iv) *Olga Tellis v BMC,* (1985) 3 SCC 545, ¶ 28, @pg 372, Vol. VI

B. COMPULSORY COLLECTION OF IDENTITY INFORMATION VIOLATES VARIOUS FACETS OF THE RIGHT TO PRIVACY

16. The limits on the coercive powers of the State are meant to constrain it from trampling on the fundamental rights of citizens. The rights in issue in the present case concern various facets of the rights to privacy and liberty that are protected by Arts. 19 and 21 of the Constitution, and arise when individuals are compelled to part with their demographic and biometric information at the point of *collection*, i.e. at the enrolment centres. These are:

(i) Bodily Privacy

17. Biometric data is part of one's body and control over one's body lies at the very centre of the right to privacy. One of the key features distinguishing free from un-free societies is the respect and sanctity accorded to the human body – "inviolability of the body" is considered to be at the heart of a free constitutional order. The body is a zone, that is accorded the highest level of protection from State intrusion, even more so than the home, because life

[4] Per **Chandrachud J., ¶¶ 103, 127 and para 297** that "The ability of an individual to make choices lies at the core of the human personality...without the ability to make choices, the inviolability of the personality would be in doubt."; per **Nariman J., ¶ 521** and **per Kaul J., ¶ 644,** "[right of] individuals to make autonomous life choices."

and liberty attaches most fundamentally to a person's body. The rights to privacy and self-determination, for example, take as their starting point, the body, and then radiate outwards into the domains of the home, correspondence, sexual expression, and so on.

[*See*: (i) ***Jordan & Ors v State,*** **(2002) ZACC 22, ¶ 81 @pg 172, Vol. II**[5]

(ii) ***S & Marper v UK*****, (2008) ECHR 1581 (GC), ¶ 81-85 @pg 227-28, Vol. II**[6]

(iii) ***Y.F. v Turkey,*** **(2003) ECHR 391, ¶ 33, @pg 248, Vol. II**

(iv) ***Leander v Sweden,*** **(1987) ECHR 4, ¶ 48 @pg 271, Vol. II**

(v) Concurrence of Blackmun J. in ***Planned Parenthood of South Eastern PA v Casey*****, 505 US 833 (1992), pg 927 @pg 370, Vol. II]** [7]

18. The inviolability of the human body rests upon two deeper premises: (a) the idea that every individual ought to be treated as an *end* in herself (and not as a means to an end), and (b) that there is an *intrinsic value* in an individual determining how and in what manner to use her body. Thus, the inviolability of the body does not become salient only in extreme situations like torture, forced sterilisations, and forced labour, but also in situations that *appear* innocuous, or at least, do not seem to present a tangible or expressible harm. The core issue then, is not whether an identifiable physical harm to the body can be pointed out, but whether the *individual's decision* about how to use her body is *taken over* by another entity (in this case the State), who decides for her instead.[8]

(ii) ***<u>Decisional Privacy</u>***

19. Decisional privacy allows individuals to make decisions about their own body, and is an aspect of right to self-determination. It is underscored by personal autonomy, which prevents the State from using citizens as puppets and controlling their body and decisions.

[*See*: (i) ***Pretty v UK,*** **(2002) 35 EHRR 1, ¶ 61, 65 @pg 444, Vol. II**

(ii) ***Selvi v Karnataka*****, (2010) 7 SCC 263, ¶ 225 @pg 559, Vol. II**[9]

(iii) Bobde J. in ***Puttaswamy*****, ¶ 424**, on the "right to choose and specify"]

---

[5] **Sachs & O'Regan JJ** concurring that continuum of privacy rights start with the inviolable inner self, move to the home, and end with the public realm; and that commitment to dignity invests great value in the inviolability and worth of the body.

[6] ***Marper*** rejected the government's arguments that fingerprints constituted neutral, objective, irrefutable and unintelligible material, holding that they contained unique information about an individual, allowing her precise identification in a wide range of circumstances. They were thus, capable of affecting private life and retention of such information without consent "cannot be regarded as neutral or insignificant".

[7] **Blackmun J.,** "*restrictive abortion laws force women to endure physical invasions far more substantial than those this Court has held to violate the constitutional principle of bodily integrity in other contexts*."

[8] To understand the centrality of the body to our constitutional scheme, consider the simple proposition that slavery is illegal under every circumstance. Our aversion to slavery is not contingent on the cruelty of slave-owners, and remains even in the case of benevolent slave masters. Our aversion, thus, is not to the physical harm the slave might suffer, but from the deprivation of their right to make decisions about how to use their body. [See **Quentin Skinner, LIBERTY BEFORE LIBERALISM, CUP, 1998, pg 39-41, 69]** [See also **McLean J.'s dissent in Dredd Scott v Sandford, 60 US (19 How.) 393 (1856) @pg 188, 195, Vol. II]**. Similarly, the compulsory collection of identity information under the Act, deprives individuals of a right to choice & control.

[9] ***Selvi*** held that there should be no scope for interference with the autonomy of an individual to make a choice about remaining silent and speaking.

(iii) Informational Privacy

20. This deals with a person's mind and comprises of (i) anonymity, (ii) secrecy, and (iii) freedom. It is premised on the assumption that all information about a person is in a fundamental way her own, for her to communicate or retain for herself as she sees fit.

[*See*: (i) Opinion of Nariman J, ***Puttaswamy*, ¶ 510**

(ii) ***R v Spencer*, (2014) 2 SCR 212, ¶¶ 38-48, @pgs 594-599,Vol. II]**

C. COMPULSION BY THE STATE VIS-À-VIS NON-STATE ACTORS

21. It is submitted that privacy rights exist both against the State and non-State actors. However, apart from the fact that the latter are defined by *consent* and *choice*,[10] there is a *qualitative difference* between the individual-State relationship, and the individual-corporation relationship, making privacy concerns vis-à-vis the former more salient.[11]

22. Thus, it is the *existence* of concentrated and centralised State power, rather than its actual or potential *use* that creates a chilling effect[12] and leads to a 'psychological restraint' on the ability of citizens to think and act freely, *per* Subba Rao. J's dissent in ***Kharak Singh v State of UP*, AIR 1963 SC 1295 @pg 133-134, Vol. III**.[13] Citizens, thus have a higher expectation of privacy from the State.

D. STATE COMPULSION, BY AADHAAR, IS NEITHER PROPORTIONATE NOR REASONABLE

23. States do not have the power to compel their citizens to do particular acts, except in a narrow range of defined circumstances. As *sentinels on the qui vive*, Courts are duty bound to protect citizens against State compulsion, whether in the context of forcibly undergoing narco-analysis/lie detectors tests [see ***Selvi*, ¶¶ 262-263 @pgs 571-572 Vol. II]** or forcible sterilisation [see ***Devika Biswas v UOI*, (2016) 10 SCC 726, ¶ 112 @pg 101, Vol. III** and the views of Chandrachud J. in ***Puttaswamy*, ¶¶ 82, 138].**

(i) Limits of compulsion by law on individual freedoms

24. The existing jurisprudence on the power of the State to compel its own citizens can illustratively be understood through three paradigms: **(a)** compulsion as *punishment* for

---

[10] Apart from the choice to opt out of technology, customers have a genuine choice in choosing the *extent* to which they will engage with technology, and a choice between service providers in a competitive big data market.

[11] For example, the maximum power that Uber can exercise over an individual is by throwing her off the Uber Platform. At this point, she can turn to other transportation service providers, such as Ola. Even if, at some future time, Uber exercised a complete monopoly over the private transportation service network, its power would still be restricted to that specific sphere.

[12] See ***Whitney v California*, 274 US 357, (*Brandeis J.* concurring), Pg. 377 @pg 136H Vol. III**

[13] See also **Laurent Sacharoff, The Relational Nature of Privacy, 16(4) Lewis & Clark L. R. 1249–1303 (2012), at 1274-80 @pg 194, 198, 200, Vol. III** identifying three harms caused by the State, in the case of a search and seizure, namely (a) intrusion harm (b) downstream harms and (c) conviction and punishment and **Quentin Skinner, "The Third Concept of Liberty", 117 *Proceedings of the British Academy* 237 at 260 (2002) @pg160, Vol. III**.

law-breaking, **(b)** compulsion in the aid of law *enforcement*, and **(c)** compulsion to *prevent* potential law-breaking.

(a) <u>Compulsion as punishment for law-breaking</u>

25. The first paradigm concerns the enforcement of legally stipulated punishments for proven law breaking. Here, the State may compel such convicts to pay a fine or send them to prison. Nevertheless, even this entitlement is subject to a threshold requirement of *proportionality*. For example, as noted by Chandrachud C.J. in ***Mithu v State of Punjab,* (1983) 2 SCC 277, ¶ 6 @ pg 231, Vol. III**, punishing the offence of theft with the penalty of cutting of hands violates Art. 21.[14]

(b) <u>Compulsion as an aid to law-enforcement</u>

26. The second paradigm concerns compulsion imposed in aid of law enforcement, and before conviction. Thus, the State may compel an accused to give fingerprints [*per* ***State of Bombay v Kathi Kalu Ogad*, (1962) 3 SCR 10, ¶¶ 10-11 @pg 272-73, Vol. III**], or specimen signatures (under **sec. 311-A, CrPC)**, or blood samples during medical examination (under **sec. 53, CrPC**).[15] Persons who have been arrested or convicted, are also required to give their measurements (including finger and footprint impressions) under **sec. 3 and 4, Identification of Prisoners Act, 1920 @pg 14-15, Vol. III.**

27. However, such powers of the State are limited and proportionate to the object sought to be achieved. Thus, in ***Selvi* ¶¶ 224-226, 255-263 @ pg 559, 569 Vol. II**, the compulsory administration of narcoanalysis, polygraph, and BEAP tests was held to be an unjustified violation of Art. 20(3) and Art. 21 of the Constitution. Similarly, sec. 7 of **Identification of Prisoners Act, 1920**[16] requires that on release (without trial or discharge or acquittal), all measurements and all photographs of the person – both copies and negatives – shall be destroyed or handed over to them, unless the Magistrate otherwise directs.

(c) <u>Compulsion to prevent law breaking</u>

28. The third case concerns compulsion to prevent law breaking, such as with preventive detention laws. It is submitted that compulsion in these circumstances is subject to the most stringent standard of judicial review and proportionality, because it effectively involves liberty infringement of persons neither convicted of, and nor accused of, a crime, and proceeds upon the mere likelihood of the possibility of future crime. Thus, in ***State of TN v***

---

[14] Similarly, while free movement of convicted persons may be restricted in prisons, convicts are not denuded of all their rights under Art. 21, per ***D. Bhuwan Patnaik v State of AP*, (1973) 3 SCC 185, ¶¶ 6,7 @pg 247, Vol. III.**

[15] *See* ***Jamshed v State of UP*, (1976) Crl LJ 1680 (All), ¶ 12-13** cited with approval in ***Selvi (supra*), ¶¶ 174, 200@ pg 544, 552 Vol. II** on extraction of blood samples under sec. 53, CrPC.

[16] See also ***MS Syed Anwar v Commr of Police*, (1991) 2 Kar LJ (Kar), ¶¶ 18-21 @pg 298, Vol. III**, that measurement or photographs of innocent persons cannot be taken under this Act "*in the guise of maintaining a history sheet*" and necessary permission from the Magistrate was required before taking such actions.

***Nabila,* (2015) 12 SCC 127, ¶¶ 12-13**, this Hon'ble Court held that the laws of preventive detention are to be strictly construed and the procedure provided must be meticulously complied with.

(ii) Limits of bodily integrity in medical jurisprudence

29. The recent judgment of ***Common Cause v UOI*, W.P (C) No. 215/2005 dated 09.03.2018** is a *locus classicus* insofar as passive euthanasia vis-à-vis Art. 21 is concerned, and has elaborated on the concepts of dignity, bodily integrity and decisional autonomy therein.[17]

30. The limits to bodily integrity have been narrowly defined in the medical context, and do not envisage a situation of compulsion, inherent in Aadhaar.[18] Thus, while DNA tests can be ordered by a Court, for instance, to reach the truth about paternity, such tests should not be ordered as a "matter of course", given privacy concerns of the individual to not submit themselves to forced medical examination (per ***Bhabani Prasad Jena v. Orissa State Commission for Women,* (2010) 8 SCC 633, ¶¶ 21-24 @pg 375 Vol. III**). They should only be ordered when an "eminent need" is established. Similarly, ***Goutam Kundu v State of West Bengal,* (1993) 3 SCC 418**, **¶ 26 @pg 387, Vol. III** held, in the context of the legitimacy of the child born during marriage, that courts cannot order blood tests as a matter of course; there has to be a strong *prima facie* case of husband's non-access, and not a roving inquiry; and no one can be compelled to give a blood sample for analysis.

31. The US Supreme Court in ***Cruzan v Director, Missouri Dept. of Health***, **497 US 261 (1990)** (**Rhenquist C.J.** in majority **at pg 269, 277-279** and & **O'Connor J.** concurring, **pg 287-88 @pg397, 405-07, 415, Vol. III)**, while holding that the State of Missouri could require "clear and convincing evidence" of a patient's wishes for removal of life support, observed that a competent person had a "*constitutionally protected liberty interest in refusing unwanted medical treatment*." The Court based its reasoning on notions of liberty being inextricably entwined with ideas of physical freedom, self-determination, informed consent; the right against unwanted medical invasion deriving from a common law right against battery; and forced treatment burdening individuals as much as State coercion.

32. Similarly, in ***Washington v Glucksberg,* 521 US 702 (1997) (Souter J.** concurring **@pg 432, 447-48, 456-57 Vol. III,** the US Supreme Court ruled that Washington law banning physician assisted suicide did not violate the 14th Amendment. However, it reiterated that the "*Constitution placed limits on a State's right to interfere with a person's most basic decisions about … bodily integrity*" since every sound adult "*has a right to determine what shall be done with his own body*". [See also ***Pretty v UK*, ¶ 63 @ p 445, Vol. II]**

---

[17] See opinion of **Hon'ble Chief Justice Misra C.J. with Khanwilkar J., ¶¶**153, 166, 176, 195(viii) at pgs 138, 153, 160, 188; **Sikri J.** ¶81, 100, 105 at pgs 254, 266, 209; **Chandrachud J., ¶**22, 80, 83, 143 at pgs 324, 373, 376, 433; and **Bhushan J.**, ¶73 at pg 507

[18] For e.g. even **sec. 90, 105, Mental Health Act, 2017 @pg 56, 63 Vol. III** circumscribe the conditions under which persons with mental illness can be admitted and treated in a mental health establishment.

(iii) ***The presumption of criminality inherent in the collection of identity information under the Act is disproportionate and arbitrary***

33. It is submitted that Aadhaar goes beyond the third paradigm of compulsion to *prevent* potential law breaking. Three factors distinguish Aadhaar from other preventive acts of State compulsion: *first*, as elaborated in **Part IV** below, Aadhaar does not follow any principles of collection/purpose limitation that ensure it is narrowly tailored with its stated aim. Identity information collected for one purpose under the Act can be used for any other (new) purpose, even by private parties u/**sec. 57**. Conversely, **sec. 15 of the Census Act, 1948 @pg 32, Vol. III**, the records of census are not open to inspection, nor are they admissible as evidence in any civil or criminal proceeding.

34. *Second*, Aadhaar treats every citizen as a potential criminal. It is akin to the creation of a national fingerprint database for the future prevention/detection of crime or saving innocent people, which is a disproportionate means of achieving a State aim [See ***MK v France*****, (2013) ECHR 341, ¶37 @pg 186 Vol. IV, ECHR** rejected government's argument that retention of fingerprints would help applicant against potential identity theft, since it would tantamount to justifying storage of information of the entire French population, which was disproportionate. In ***S & Marper*****, ¶¶ 112, 119-121, 123 @pg 235, 237 Vol. II** rejecting the government's justification for the retention of fingerprints since future prevention of crime was very widely worded, without guarantees against arbitrariness and irrespective of guilt.]

35. Such pervasive presumptions were also reflected in the infamous sterilisation opinion in ***Buck v Bell*****, 274 US 200 (1927) @pg 467, Vol. III,** that "*Three generations of imbeciles are enough*", which, while not formally overruled, was distinguished out of existence in ***Skinner v. Oklahoma*****, 316 US 535 (1942), @pg 469, 473, 475, Vol. III.**

36. *Third*, Aadhaar does not require the State to have a *reasonable belief* that a said individual might be committing a crime or perpetrating identity fraud, much less require a judicial determination to that effect. Thus, the compulsion exercised under Aadhaar is more disproportionate than even the most stringent preventive detention law, since it does not require any standard of suspicion before its compulsion comes into play. It also goes far beyond the accepted standards for *preventive deprivation* of rights, such as "spark in a powder keg" for free speech (see ***Rangarajan Etc vs P. Jagjivan Ram*****, (1989) 2 SCC 574, ¶45 @pg 504, Vol. III),** which builds in safeguards to limit restrictions.

(iv) ***Absence of safeguards: Lack of judicial/ independent oversight during enrolment***

37. The **Bombay Habitual Offenders Act of 1959** also requires *fingerprints for preventive purposes*. **Sec. 3** authorises the State Government to maintain a register of "habitual offenders", whose finger and palm impressions, foot-prints and photographs may be taken by District Magistrate, after giving them reasonable opportunity of showing cause why such an entry should not be made. Such persons shall also have the right to make a

representation against such an order [See **sec. 4(c) proviso r/w sec. 6 r/w sec. 10 @pg 36, 38, Vol. III]** Thus, the Act requires (a) objective reasonable grounds of suspicion, which are made out by the fact of three convictions; (b) pre-compulsion hearings before taking preventive coercive action; and (c) supervision and oversight.

38. In the case of Aadhaar, however, biometric data of all individuals is *collected* by enrolment agencies, who are private entities [**Regulation 23, Enrolment Regulations]** (a) without requirement of reasonable suspicion, (b) without requiring independent/judicial application of mind and without any oversight, and (c) without any principles limiting the storage or use of such sensitive data in the CIDR. [See ***S & Marper*, ¶ 99, 119 @pg 232, 237, Vol. II** on need for independent oversight.][19] Thus, the Aadhaar Act is not narrowly tailored, proportionate, or reasonable. In fact, it mandates the State to commit a crime for the purpose of detecting a crime[20] [See ***Minerva Mills v UOI*, (1980) 3 SCC 625, ¶ 56-57 @pg 594, Vol. III** on purity of means and ***Puttaswamy*, ¶ 125, 265-267]**

39. It is apposite to remember the words of **Khanna J.** in his dissent in ***ADM Jabalpur v Shivkant Shukla*, (1976) 2 SCC 521,** while cautioning against over-zealous governments

> "**529**… experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded persons. Greatest danger to liberty lies in insidious encroachment by men of zeal, well-meaning but lacking in due deference for the rule of law."

40. In a similar vein, Frankfurter J.'s dissent in ***Davis v U.S.*, 328 US 582 (1946), at 597 @pg 634, Vol. III** bears reiteration:

> "It is easy to make light of insistence on scrupulous regard for the safeguards of civil liberties when invoked on behalf of the unworthy. It is too easy. History bears testimony that by such disregard are the rights of liberty extinguished, heedlessly at first, then stealthily, and brazenly in the end."

E. THE ACT IS UNCONSTITUTIONAL SINCE IT COLLECTS THE IDENTITY INFORMATION OF CHILDREN BETWEEN 5-18 YEARS WITHOUT PARENTAL CONSENT

41. The enrolment of children between 5-18 years is being conducted without the requirement of parental consent, and without providing for any opt-out measure after the children turn 18 years [**see sec. 5 r/w Regulations 5 r/w 10(4)(a) r/w Schedule III of Enrolment Regulations**].

---

[19] See also ***X v Finland*, (2012) ECHR 1371, ¶ 220 @pg 559, Vol. III** that decision making that seriously interferes with a person's physical integrity must have guarantees against arbitrariness, including providing for judicial scrutiny and recourse to a legal remedy

[20] See also **Brandeis J.'s dissent, *Olmstead v US*, 277 U.S. 438 (1928) at 485 @pg 613, Vol. III** cautioning against the government becoming a lawbreaker (by relying on ends to justify its means in securing administration of criminal law), and the resultant contempt it would breed for the law and ***S & Marper* ¶ 112 @pg 236, Vol. II** that protection afforded by Art. 8 would be "unacceptably weakened" if modern scientific techniques in criminal justice system were allowed "at any cost and without carefully balancing… against private life interest"

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

42. It is submitted that, at the point of storage, the Act violates the right to privacy: *first*, the centralised storage of identity information in the CIDR is disproportionate; *secondly*, the long period of retention for such data and authentication logs is disproportionate; *thirdly*, the absence of a right to access or correct one's biometric information infringes Arts. 19 and 21; and *fourthly*, the Act lack procedural safeguards to secure the data, once collected. In fact, a close reading of the Act shows that there is no specific statutory backing for centralised storage and the aspect of storage should fail on the grounds of want of law also.

A. CENTRALISED STORAGE OF IDENTITY INFORMATION IS DISPROPORTIONATE

43. The Aadhaar Act proceeds on the basis of permanent, centralised storage of demographic and biometric data of every resident. In contrast, other laws (such as the Identification of Prisoners Act, Census Act, or the Passports Act) store personal data in "silos" and are not linked to other identity records. Further, in the absence of any law to prohibit the 'seeding' of various databases that are linked through the Aadhaar number, the centralised storage and use of such sensitive personal information facilitates profiling and surveillance.

44. It is submitted that the *mere* storage and retention of personal data is a violation of the right to privacy [***Leander*, ¶ 48 @pg 271, Vol. II; *MK v France*, ¶37 @pg 186, Vol. IV**]. Its subsequent use/abuse has no bearing on this finding [***Amann*, ¶ 69 @pg 308, Vol. II; *S & Marper*, ¶ 121 @pg 237, Vol II].** Hence, the retention of data in CIDR is disproportionate.

B. UNDULY LONG RETENTION PERIOD OF TRANSACTION DATA AND AUTHENTICATION RECORDS IS DISPROPORTIONATE

45. **Regulation 26 of the Authentication Regulations** envisages the storage and maintenance of authentication transaction data by the UIDAI, including metadata related to the transaction, authentication requests, response data sent and received. It is now well settled that metadata reveals much more about an individual than the content of data itself. Thus, the **proviso to Regulation 26** that the UIDAI shall not store the *purpose* of authentication, is no safeguard. Further, **sec. 8(4) of the Act** expands the definition of "authentication" from **sec. 2(c)** to allow UIDAI to respond to authentication queries with positive, negative, "*or any other appropriate response sharing such identity information excluding any core biometric information*". Pursuant thereto, **Regulations 2(1)(j) r/w 2(1)(k) r/w 3 of Authentication Regulations** has enabled the UIDAI to return the entire demographic data and photograph (known as e-KYC data) in an authentication query.

46. The storage, archiving, and retention of the Petitioners' authentication records or transaction data by the UIDAI for five years (under **Regulation 27, Authentication Regulations**) and by the requesting entities (R**egulation 18(3)**) and Authentication Service Agencies (**Regulation 20(3**)) for *minimum* of seven years is wholly disproportionate. Further, the lack of safeguards to protect confidentiality of the data or guidelines for

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

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

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

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

48. The citizen's right to know, derived from Arts. 19(1)(a) and 21, includes the right to receive information, [22] and hence, access and control one's own personal data. The globally accepted privacy principles, as recognised by the **Report of the Group of Experts (2012) @pg 7, 17 Vol. IV,** include such a right to "access and correction", which confers in every individual a *right* to (a) access their personal data; (b) correct, amend or delete inaccurate information; and (c) know the nature of personal information stored by data controller.

49. However, the Aadhaar Act and accompanying Regulations deprive Aadhaar number holders of the right to access and correct their personal information. At the outset, the proviso to **sec. 28(5)** of the Act denies individuals the right to access *their own* core biometric information stored in the CIDR. This amounts to an impermissible waiver of rights under Arts. 19(1)(a) and 21 since it divests Aadhaar number holders from any modicum of control over their information [See ***Baseshshar Nath v CIT*, AIR 1959 SC 149, ¶ 12-15 @pg 260, 263 Vol. IV and *Puttaswamy*, ¶ 126**].

50. Despite recognising some right to access information under **sec. 3(2)(c**) and authentication records under **sec. 32(2)**, the Act and Regulations do not provide any measure by which such rights can be enforced:

---

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

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

(a) **Regulation 9(c) of Enrolment Regulations** states that the Aadhaar number holder has a "right to access information", with the procedure for making such requests for access provided in Schedule I. However, **Schedule I** only states, "*I have a right to access my identity information (except core biometrics) following the procedure laid down by UIDAI*". Thus, despite cross-citing each other, no procedure is laid down.

(b) **Regulation 3(3) of Sharing of Information Regulations** states that the UIDAI "shall" share authentication records of the Aadhaar number holder with them in accordance with **Regulation 28 of Authentication Regulations**; which in turn states that the right to access authentication records is "subject to conditions" prescribed by the UIDAI. Further, **Regulation 28(1**) grants the right to access one's authentication records "*within the period of retention of such records before they are archived*", which as per **Regulation 27(1) is** only 6 months. Thus, even though an individual's authentication transaction data is "archived" by the UIDAI for five years (after the expiry of the 6 month period), she is only entitled to access it during the 6 months.

(c) **Regulation 4(3) of Sharing Regulations** states that private requesting entities "may" share the authentication logs of an Aadhaar number holder with them upon their request, with no recourse to the Aadhaar number holder if such a request is denied.

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

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

52. This Hon'ble Court in ***Puttaswamy* [per Kaul J., ¶ 638**] and earlier in ***A.K Roy,* (1982) 1 SCC 271, ¶ 35 @pg 340, Vol. IV** made it clear that for any law to be constitutionally valid, it must contain certain minimum procedural guarantees, to ensure due process and reasonableness under Art. 21.[23] However, the Act and Regulations do not contain such minimum guarantees, and thus, fail the test under Art. 21 of the Constitution.

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

[23] See ***Dr N.B. Khare v State of Delhi,* [1950] SCR 519 @pg386, Vol. IV** *and* ***PUCL v UOI,* (1997) 1 SCC 301, @pg 415, Vol. IV** in the Indian context. See ***S & Marper,* (supra), ¶ 99, 103 @ pg 232-33, Vol. II**; ***X v Finland,* (supra) ¶ 220-21 @pg 559, Vol. III; *Peruzzo & Martens* (supra), ¶ 47 @pg 205, Vol. III; and *Z v. Finland,* (1997) ECHR 10, ¶ 95, 112, 114 @pg 439, 444-45, Vol. IV** for ECHR.

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

54. It is now well-recognised that centralised biometric databases are not secure, and the Aadhaar infrastructure, in particular is susceptible to data breaches, especially due to its use of biometrics as authentication credentials. Such concerns also led to scrapping of a similar project in the UK.[24]

55. Unlike a credit card or financial transaction, breach of biometric information cannot be reversed. More egregiously, the Aadhaar Act does not include a data breach notification principle, as recommended by the **Report of the Group of Experts (2012) @pg 16, Vol. IV**, to inform the Aadhaar number holder of any breach of personal data.

56. Further, **Regulation 4(2)(b) of the Authentication Regulation** recognises the OTP-based mode of authentication, which is also used under the e-KYC authentication facility u/**Regulation 3(ii).** OTP authentication is often used when biometric authentication fails. However, OTP authentication defeats the objective of preventing identity fraud, since all it requires is a phone number and/or email address, which, as per **Regulation 4(2)(i) read with 10(5) read with Schedule III of the Aadhaar Enrolment Regulations** need not be registered and verified at the time of getting an Aadhaar.

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

57. Fundamental rights are violated at the point of use of identity information under the Act in two ways. *First*, the legal framework to govern the manner in which personal data might be used lacks purpose limitation, limited disclosure and permits use by private entities. *Second*, the mandate of sec. 7 of the Act to use Aadhaar as a compulsory form of identification and authentication for availing entitlements violates Art. 14 & 21, since by design, it is exclusionary, arbitrary and disproportionate.

A. THE LEGAL FRAMEWORK OF THE AADHAAR ACT THAT GOVERNS THE USE OF INFORMATION FAILS TO MEET CONSTITUTIONAL STANDARDS

(i) The Act lacks any purpose limitation

58. Two key inter-related principles of privacy relate to collection and purpose limitation, which require a data controller to *collect* only such data as is necessary for the identified purpose; and to then process and *use* such collected data only for the stated purpose and

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

after taking informed consent [See ***Puttaswamy,* ¶314.3-314.4** and **Report of Group of Experts, @pg 6, 17, Vol. IV].** However, the Act violates both these principles.

59. The Act emphasises the continued use of Aadhaar number as a unique identifier. There is nothing to limit the use of collected data only to the (original) stated purpose and only after (re)-taking the consent of individuals. By contrast, the US Department of Homeland Security issued **Privacy Policy Guidance Memorandum on 04.06.2007 @pg 59, Vol I** stating that, as a general rule, it "*shall not collect or use an SSN as a unique identifier*…..".

60. Thus, in terms of necessity and proportionality, Aadhaar is significantly different from other situations where the State requires an individual's biometrics, such as for passports, and under the Registration Act. The requirement in these cases is *one-time,* and for a specific purpose identified in advance. Conversely, Aadhaar is an *open-ended general purpose vehicle*: the *point* at which a person enrols for Aadhaar is entirely delinked from the range of entitlements that Aadhaar is, or can subsequently be, made compulsory for. [See **S & Marper, ¶82 @pg 228, Vol. II** that Art. 8 concerns did not arise when photographs were not entered into a data processing system and the authorities had not attempted to identify the person through data processing.] Thus, the compulsion in the taking of person data under the Aadhaar Act is entirely different in nature, scale, and degree, from the compulsion that exists under other laws.

(ii) ***The Regulations governing the use of the stored identity information are vague***

61. **Section 3(2)(a)-(b)** of the Act requires the enrolling agencies to inform the individual undergoing Aadhaar enrolment about the "manner in which information shall be used" and the "nature of recipients with whom the information is intended to be shared during authentication". However, the Enrolment Form in **Schedule I of Enrolment Regulations** does not stipulate any such mechanism. Thus, the Act and Regulations are completely vague on the purpose for which the information being collected *can be* used. There is no contemporaneous documentation in the Act to evidence the mode and manner, and whether at all there is, of compliance with this Act. It is settled law that a person cannot be deprived of her liberty by a law, which is nebulous and uncertain in its definition and application [per ***A.K. Roy* (1982) 1 SCC 271, ¶ 61 @p. 356, Vol IV].**

62. The Act is also contradictory. While **s. 29(1)** of Act states that core biometric information can never be shared, this is expressly contradicted by **s. 29(4),** which states that core biometric information can be published in a manner "as may be specified by regulations". This conflict between sec. 29(1) & (4) is irreconcilable and liable to be struck down.

(iii) ***Section 33 of the Act governing the disclosure of information in certain cases is disproportionate, contrary to principles of natural justice, and unconstitutional***

63. The Act legitimises mass surveillance by the State, which is antithetical to the principles of democracy. **Sec. 33(2)** gives a *carte blanche* to the State to access/use/disclose identity information of individuals, including their core biometric information, "in the interest of

national security". This functions as a blanket exemption from confidentiality obligations and sharing restrictions, without providing any safeguards whatsoever, and is beyond even the limitations imposed by this Hon'ble Court in the context of telephone tapping in ***PUCL v UOI,* (1997) 1 SCC 301, ¶35 @ pg 415, Vol IV.**

64. More particularly, there is **(a)** no requirement to consider the existence of alternative means of acquiring information; (**b)** no overall time limit set under sec. 33(2) for which the direction thereunder shall be valid; (**c)** no requirement for maintenance of records; (**d**) no limitations on use of obtained material; and (**e**) no requirement to destroy the data once it is no longer necessary for "national security". Apart from this, the Act does not define "national security" and does not require any *ex-ante* or *ex-post* independent oversight.

65. The absence of safeguards, especially judicial/parliamentary oversight or fixed time limits, is in contrast to even proceedings under preventive detention or surveillance, and is not just, fair, or reasonable. Thus, sec. 33(2) is disproportionate, and violative of Art. 21.[25]

66. Principles of natural justice are further given a go by in **sec. 33(1)** of the Act, which permits the disclosure of identity information or authentication records of individuals, pursuant to a judicial order, after hearing the UIDAI. No *ex ante* or *ex post* hearing is given to the concerned Aadhaar number holder, nor the reason for which such information is sought, nor any guidance given to the Court for exercising its powers [See ***Leander v Sweden*, ¶ 51, 62, 64 @ pg 272, 275 Vol II** in a national security context]

(iv) ***<u>The use of the Aadhaar infrastructure by private entities is unconstitutional</u>***

67. **Sec. 57** has enabled private companies to avail the authentication facility under **sec. 8(4)** and access identity information stored in the CIDR, which in unconstitutional.

68. *First,* authorising the use of the "Aadhaar number" as the sole proof of identity for an open-ended and unspecified set of "laws" or "contracts", defeats the principle of informed consent at the time of enrolment. Further, the duty to seek consent under **sec. 8** to undergo authentication is entirely illusory, due to the threat of discontinuation of service/benefits. In any event, there can be no waiver of fundamental rights *per* ***Baseshar Nath*, ¶12-15 @pg 260-263, Vol. IV.** *Secondly*, the broad and unlimited scope of activities covered under **sec. 57** and the kinds of private entities permitted to use Aadhaar is entirely disproportionate, beyond the Aims & Objectives of the Act, and without any compelling State interest. The Act also fails to specify the *purpose* for which the Aadhaar number may be used to establish identity, and whether it is *necessary*, given the alternative, existing modes of identification. *Finally*, no procedural safeguards govern the actions of private entities, and no remedies exist for authentication failures or service denial.

---

[25] See ***Secy of State v Watson*, [2018] EWCA Civ 70, ¶13 @p 147, Vol V,** where the Court held the Government's mass data retention regime unlawful for lack of effective safeguards, i.e. absence of prior or independent review/ authorisation on access to data, or a limit on the use of data to serious crime. See also ***Leander v Sweden*, ¶ 60, 65 @ pg 275, Vol. II** and ***Amann v Switzerland*, ¶ 60-61 @ pg 306, Vol. II** for judicial or legislative oversight.

B. SECTION 7 OF THE AADHAAR ACT IS UNCONSTITUTIONAL AND VIOLATES ART. 14

69. It is submitted that the requirement under **sec. 7** for every person to undergo authentication to avail benefits/services/entitlements, falls foul of Art. 14 since, *first*, such mandatory authentication has caused, and continues to cause, exclusion of the most marginalised sections of society; and *secondly*, this exclusion is not simply a question of poor implementation that can be administratively resolved, but stems from the very *design* of the Act, i.e. the use of biometric authentication as the primary method of identification.

(i) Factual foundation: Systematic exclusion caused by Aadhaar

70. Vide Government Notification S.O. No. 371(E) dated 08.02.2017, proof of possession of an Aadhaar or enrolment number or undergoing Aadhaar authentication is a mandatory pre-requisite for receiving subsidised food grain under the National Food Security Act. [See also **Reply to Lok Sabha Unstarred Qs No. 2477 dated 02.01.2018 @pg 1, Vol. VI]** In this "Aadhaar-Based Biometric Authentication" ["**ABBA"]** system, a Point of Sale ["**POS**"] machine is installed with a fingerprint reader to authenticate persons monthly, when they go to access their entitlement [See **Jean Dreze *et al,* "Aadhaar and Food Security in Jharkhand: Pain Without Gain?", 52(50) EPW (2017) @pg 3, 6 Vol. VI].**

71. Successful monthly authentication is contingent on harmonious working of all attendant Aadhaar processes and technologies – i.e. correct Aadhaar-seeding, successful fingerprint recognition, mobile and wireless connectivity, electricity, functional POS machines and server capacity – each time. It is also dependant on age, disability (e.g. leprosy), class of work (e.g. manual labour), and the inherently probabilistic nature of biometrics.

72. **Para 9.76** of the **Economic Survey of India 2016-17 @pg 23, Vol. VI** reports that authentication failures have been as high as 49% in Jharkhand and 37% in Rajasthan, recognising that "*failure to identify genuine beneficiaries results in exclusion error*". The reasons for authentication failure in Rajasthan were elaborated in **Reply dt. 09.08.2016 to Rajya Sabha Unstarred Qs No. 2566 @pg 44-45, Vol. VI**. Other field studies and surveys have also demonstrated the growing authentication failure rates, leading to further marginalisation and death.[26]

73. It is submitted that the requirement of periodic, biometric authentication has created an "undue burden" on the citizens, which is unconstitutional [See ***Planned Parenthood* @pg 346, 354 Vol. II** on "undue burdens" and "substantial obstacles" caused by the spousal notification requirement and ***Whole Woman's Health v Hellerstadt,* 136 S.Ct. 2292 (2016)** at **2300**, **2321 @pg 67, 88 Vol. VI**, striking down the Texas abortion House Bill since it did "*little or nothing else for health, but rather strew impediments to abortion*", was and undue burden on abortion access, and violated the Constitution]

---

[26] See (a) **Affidavit of Reetika Khera dt. 04.01.2018 @pg 25-36, Vol. VI;** (b) **Anmol Somanchi *et al,* "Well Done ABBA?", 52(7) *EPW* (2017) @pg 39, Vol. VI;** (c) **Jean Dreze (supra) @pg 2, 6, Vol. VI;** (d) **Articles in *Scroll.in* @pg 46-52 Vol. VI** & (e) ***Indian Express* @pg 53-54 Vol. VI** for more details.

(ii) Design and operation of the Aadhaar program is inherently arbitrary

74. The State's contention that exception handling mechanisms [**Circular dt. 24.10.2017 @pg 57-58, Vol. VI**] have resolved implementation issues is incorrect and untenable since, *first*, the constitutional violation lies in the inherent design of the Act, and *secondly*, violations of rights cannot be left to administrative vagaries. It is submitted that a law can be struck down as arbitrary, if there is no determining principle, it is excessive & disproportionate [See ***Shayara Bano v. UOI* (2017) 9 SCC 1, ¶ 5, 87, 101 @pg 124, 175, 183, Vol. VI** and ***Independent Thought v UOI*, (2017) 10 SCC 800, ¶ 100, 166-70, 175 @pg 238, Vol. VI]**

(a) Reliance on a probabilistic system of biometric authentication is arbitrary

75. *First*, determination of legal entitlements is *contingent* on a positive authentication response from the UIDAI. Biometric technology does not guarantee 100% accuracy and is fallible, with inevitable false positives and false negatives that are design flaws of such a probabilistic system.[27] [See ***Planned Parenthood*, @pg 354, Vol. II** on the focus of constitutional inquiry having to be the group of women for whom the law is a restriction and is irrelevant] Further, biometrics also change over time, a fact expressly recognised by **sec. 31(2)** of the Act. However, it places the entire burden of deducing that one's biometric information has changed, and then having it altered, on the individual, even though literacy, including knowledge of technology in this country is negligible.

76. *Second*, classification under the Act lacks rational nexus. The entitlement of an individual depends upon status, and not proof of identity. Nevertheless, at the point of use, ABBA divides residents into two classes: those who have and do not have Aadhaar; and those who authenticate successfully, and those who do not. The probabilistic nature of biometrics means that this division bears no rational nexus with the question of status for receiving benefits. It leads to under-inclusion, and is thus arbitrary, causing an Art. 14 violation.

77. It is further well settled that the validity of an act is to be judged not by its object or form, but by its direct *effect* on fundamental rights [See ***State of Bombay v Bombay Education Society*, (1955) 1 SCR 568, ¶16 @pg 250-52, Vol. VI** and ***Bennett Coleman v UOI*, (1972) 2 SCC 788**, **¶¶ 39, 41 @ pg 273F, Vol. VI**]. Given that the probability of biometric mismatch is greatest for the aged, disabled, and individuals engaging in manual labour – amongst the most vulnerable sections of society – the decision to use periodic biometric authentications has a direct and disparate effect of violating fundamental rights of this class [See ***Madhu v Northern Railways*, (2018) SCC Online Del 6660 (DB), ¶¶17-30].**

---

[27] See **National Research Council in Washington DC Report, "Biometric Recognition: Challenges and Opportunities" (2010) @pg 297, Vol. VI** in the context of biometrics, "*human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated.*" Notably, even as per **UIDAI's own Report on "Role of Biometric Technology in Aadhaar Enrolment" (2012) @pg 285-286, Vol. VI,** the biometric accuracy after accounting for the biometric failure to enrol rate, false positive identification rate, and false negative identification rate, was 99.768% accuracy. For a population of over 119.22 crore enrolled in Aadhaar, it is a shocking admission of the fact that there are 27.65 lakh people who are excluded from benefits linked to Aadhaar.

78. *Third,* the denial of legal entitlements of an individual takes place at the level of the ration dealer, where an unsuccessful biometric authentication leaves an individual with no right of hearing or a review. The lack of accountability and remedies against the UIDAI for such wrongful denial of legal entitlements and the absence of any judicial supervision, is manifestly arbitrary and violative of Art. 14. Notably, despite specifically designating various actions as criminal offences, **sec. 47** only permits the UIDAI to initiate criminal prosecution, and eliminates the involvement of the Aadhaar number holder entirely, which is contrary to the dictum of this Hon'ble Court in ***Anita Kushwaha v Pushp Sudan,*** **(2016) 8 SCC 509, ¶ 31 @pg 331, Vol. VI.**

(b) <u>Violation of rights cannot be left to vagaries of administrative discretion</u>

79. The State has argued that the exclusionary effects of ABBA have been mitigated by a combination of sec. 7 of the Act and various notifications, which permit residents to only show proof of Aadhaar Number or provide another form of identification, to continue to avail benefits. Thus, the stand of the State is that Aadhaar is not a *mandatory*, but only a *primary* form of identification, with other options, should it fail. However, this Hon'ble Court has held in ***State of UP v Johri Mal,*** **(2004) 4 SCC 714 ¶86 [cited in *State of UP v Ajay Kumar Sharma,* (2014) 3 SCC 568, ¶ 6 @pg 397, Vol. VI]** and ***Shreya Singhal v UOI,*** **(2015) 5 SCC 1, ¶95-96 @pg 421-422, Vol. VI** that law cannot be substituted by executive instructions which may be subject to administrative vagaries, and an unreasonable statute cannot be saved by being administered in a reasonable manner.

80. It is both irrational and arbitrary to provide alternatives to ABBA, by way of circulars, *at the point of failure* of authentication (rather than *before* such point), when the determination of legal entitlements and responsibility for allowing the use of an alternative rests in the hands of private parties (e.g. fair price shop owner or POS machine operators). In fact, the circulars are a clear indicia that biometric authentication under Aadhaar is not mandatory, and illustrate the disproportionate nature of the authentication condition. At the very least, biometric authentication, as the *sole* proof of identity may be made voluntary.

C. SECTION 7 OF THE AADHAAR ACT IS UNCONSTITUTIONAL AND VIOLATES ART. 21

81. The requirement to undergo mandatory authentication to access legal entitlements is not just, fair or reasonable under Art. 21. The State's justification of plugging welfare leakages, apart from being erroneous and failing the proportionality test, falls short of discharging the burden expected of it.

(i) <u>Mandatory authentication at the point of use violates Article 21</u>

82. The right to food, recognised as a constitutional right under Art. 21 r/w Art. 39A and Art. 47 of the Constitution (per **PUCL v UOI, (2013) 2 SCC 688, ¶¶ 6, 7 @pg 429, Vol. VI**), is also a statutory right under the **National Food Security Act 2013**. Similarly, the right to health/pensions are constitutional/ statutory rights, which are not predicated on having only *a* particular form of identification. These are entitlements of the citizens, and are not

largesse given by the State as part of its "welfare" program. Given that ABBA alters the entire design & institutional structure through which residents were receiving entitlements, mandatory imposition of Aadhaar violates their rights to *choose how to identify themselves to the government in a reasonable and non-intrusive fashion.*

83. **Salmond** lists five characteristics that inhere in every "legal right". Of these, it is important to note that (**a**) The right is vested in a person, who is the person *entitled* and subject of the right; (**b**) The right avails against a person, on whom lies the *correlative duty,* and who is the subject of the duty; (**c)** The right *obliges* the person bound to an *act* or omission in favour of the person entitled, which is the "content" of the right. [See **P.Z. Fitzgerald, *Salmond on Jurisprudence,* 12th edn, (1966) at pg 221 @pg 436 Vol. VI]** Thus, the State is the facilitator and guarantor of fundamental rights.

84. However, through the insistence on mandatory, monthly authentication, the State has, at its own will, created various obstacles and altered the rights and legal relations of its citizens. In doing so, it has converted the *right-duty* paradigm to a *power-liability* paradigm, where its exercises of "authority" – in using a probabilistic technology – will determine if citizens will be able to avail their "legal rights" (in the wide sense of the term). Instead of the citizen's *right* to food, imposing a correlative *duty* on the State to take action to ensure the proper fulfilment of such rights, the State is exercising its *power* to convert the constitutional rights of its citizens into *liabilities* (**pg 228-230 of Salmond @pg 443-445 Vol. VI]**).

85. In an analogous context, it is helpful to see the observations of this Hon'ble Court in ***Suk Das v UT of Arunachal Pradesh*, (1986) 2 SCC 401, ¶ 6 @pg 455 Vol. VI**, that fundamental rights cannot lawfully be denied, if applicants do not apply for free legal aid. The Court took into consideration the extent of poverty, illiteracy and lack of legal literacy in India, concluding that requiring accused to *ask* for free legal services would render legal aid a paper promise. These observations are relevant in the present case, considering that the government notifications, creating exceptions, are an "idle formality".

(ii) <u>The government has failed to discharge its burden of proof under Art. 21</u>

86. Having established the infringement of Art. 21, the burden shifts on the State to justify such an infringement. It is submitted that the State's primary justification – of eliminating welfare leakages and ensuring "better targeting"[28] – does not stand up to judicial scrutiny. *First*, it has failed to discharge its burden of showing that the purported leakages were exclusively caused due to identity fraud, and that those leakages would not exist if Aadhaar is implemented. In fact, a close reading of the affidavit dt. 16.01.2018 filed by the State shows that the predominant loss due to leakage is caused due to misappropriation, loss in transit, loss in storage, non-accounted stock, loss due to employees' mistake, loss due to bulk diversion from godowns, and loss due to high transaction costs. Further, the counter

[28] See **pgs 7-44 @ paras 12, 16 of additional affidavit filed by Union of India dated 16.01.2018**

affidavit states that the loss has been primarily due to "eligibility" and "quantity" fraud. Even in case of losses due to identity fraud, the State has not given any empirical data. In fact, on the aspect of bogus ration cards, it has taken into account cancellations due to the fresh issuance of ration cards and counted those towards identity fraud. Not a single case of any imposter of having been caught and a criminal case registered has been set out in the counter. It is impossible that diversions of such large magnitude can happen due to identity fraud when the quantity given to an individual is in the range of 5kg per month, unless there is a huge cartelisation and conspiracy in large scale printing of bogus ration cards. If so, there would have been criminal cases registered. Thus, the reasons adduced by the State are neither relevant, nor sufficient, to justify the introduction of Aadhaar, and it is eminently permissible for a Constitutional Court to review the assessment of the State to see whether it comports to Art. 21. *Secondly*, it has failed to show how the introduction of Aadhaar will stop the losses causes on any of the grounds above. While both in the pre- and post-Aadhaar scenario the human element continues, in fact, in the post Aadhaar scenario, with the introduction of the machine, the vendor has ben greatly empowered for further mischief, and the vendee has been rendered completely helpless.

(a) <u>Proportionality, burden of proof, standards of review</u>

87. The requirement of proportionality stipulates that the *nature and extent* to which the State interferes with the exercise of a right (in this case, the rights to privacy, dignity, choice, and access to basic entitlements) must be proportionate to the *importance* of the goal it is trying to achieve (in this case, purported plugging of welfare leakage and better targeting). In applying the proportionality standard, a Court is not expected to mechanically defer to the State's factual assertions, and given the intrusive nature of regulation herein, the usual judicial deference to legislature is inappropriate. [See **Powell J.** in ***Moore v City of East Cleaveland,* 431 US 494 (1977) @pg 461 Vol. VI** and ***S & Marper,* ¶ 101, 102 @ pg 233, Vol. II.** On the application of compelling State interest test, see ***Gobind v State of MP,* (1975) 2 SCC 148, ¶22 and 31**].

88. In the present case, the Petitioners submit that the State has failed to discharge its burden of demonstrating the need for biometric authentication, because:

a. The forced commandeering of the human body and presumption of criminality represents a serious infringement of rights, and accordingly, as demonstrated above, requires a very <u>high burden</u> of justification from the State;
b. The State's assumptions use <u>faulty</u> methodology, consequently, inflating the <u>savings</u> claims, and resulting in the State failing to discharge its burden;
c. The State has failed to demonstrate that <u>other, less invasive ways</u> would be *significantly worse* at addressing the problem, especially given recent studies that found a significant reduction in PDS leakages, due to innovations devised to work within the PDS system;
d. The absence of proportionality is further established by the fact of <u>systematic exclusion</u>;

e. The entire design and operation of the Aadhaar program is inherently arbitrary, which along with the aforesaid exclusion, demonstrates that the use of Aadhaar *perpetuates* infringement of rights instead of protecting them.

(b) Failure to demonstrate that Aadhaar has caused significant savings – illustrated in the PDS Scheme

89. Three different frauds exist in PDS. The first, "**eligibility fraud**", is when ineligible persons, manage (through the use of fudged documents or other forms of corruption) to get themselves included as recipients for a welfare scheme. "**Quantity fraud**" refers to situations where eligible persons receive less than their due entitlements, for e.g., due to under-selling.[29] "**Identity fraud**" occurs where a person fraudulently claims an eligible person's benefits, as a "ghost" (by getting a ration card in the name of a non-existent/dead person) or "duplicate" (by getting two cards made for one person). ABBA, at best, can *only* help in reducing identity fraud. An Aadhaar number has no bearing on the question of status or entitlement to benefits. Thus, an intended beneficiary will still require a ration card (or other proofs of eligibility), but will now have the added burden of hoping for a successful authentication under the probabilistic ABBA [*See* **Reetika Khera, *Impact of Aadhaar in Welfare Programmes*, 52(50), EPW 61, at 62 @pg 488-489 Vol. VI**].

90. There are four incorrect assumptions in the government's savings claim justifying the introduction of Aadhaar. *First*, its affidavit assumes, contrary to the studies annexed therein, that the leakages problem is caused solely due to identity fraud. The studies show that eligibility and quantity frauds are the substantial cause for leakages, which are not even addressed by Aadhaar.[30]

91. *Second*, no single study demonstrates that identity fraud is a large proportion of corruption in the welfare system, whereas there is evidence that quantity fraud is pervasive.[31]

92. *Third*, the government's claims of savings, *inter alia* of Rs. 14,000 crores[32] in the PDS system, due to the deletion of 2.33 crore ration cards is incorrect, inflated, and based on wrong assumptions since **(a)** it admittedly does not have estimates of leakages in PDS,[33] nor has any study been done to see if POS machines are effective in removing PDS

---

[29] **Eligibility fraud** covers those who do not qualify as a "priority household" under the National Food Security Act, 2013, and are not eligible for the 5kg of food grain per person per month, but manage to get themselves included. **Quantity fraud** covers situations where a person is forced by the Fair Price Shop owner to sign off as having received 5 kg of food grain, even though they actually received only 3 kg.

[30] See **pgs 8, 9, 12, 15, 18, 25, 27 of additional affidavit filed by Union dt. 16.01.2018**

[31] See (a**) Reetika Khera affidavit @pg 26, Vol. VI;** (b) **Jean Dreze and Reetika Khera, "Recent Social Security Initiatives in India", 98 *World Development* 555, at 563 (2017) @pg 505-507 Vol. VI (c) Jean Dreze (supra) @pg 8, Vol. VI**

[32] See **para 10(a)(iii) at pg 31 of counter filed by UOI dt. 23.09.2015 in WP(C) No. 342/17 & 797/16**

[33] See **Reply dated 13.03.2015 to Unstarred Qs No. [1846] in the Rajya Sabha @ pg 570, Vol. VI**

irregularities[34] **(b)** it conflates issue of "bogus /ineligible ration cards" (eligibility fraud) with identity fraud; **(c)** the figure of 2.33 crore includes West Bengal, where ration cards are issued to each person, as opposed to each household; **(d)** a large number of these 2.33 crore cards were deleted even before Aadhaar-integration and seeding came into effect;[35] (**e)** the savings figure includes even those eligible beneficiaries who have been removed from the list due to failure to link Aadhaar properly[36] and (**f)** it does not value the cost of loss of privacy. Most importantly, the basis for reaching such savings figure has not been disclosed. [See also ***Marper*, ¶ 115-16 @ pg 236, Vol. II** on misleading statistics**]**

93. *Fourth*, it is now evident[37] that ABBA has given new powers to POS operators and plausible deniability for corrupt practices. Thus, the entire premise of Aadhaar for targeted delivery has not been accomplished, while actually perpetuating the power of middlemen.

94. *Finally*, the government relied on various old studies such as the CAG Audit Report, 1999; NIPFP's Report on Budgetary Subsidies in India, 2003; or World Bank's Report on India's PDS, 1997, even though there had been a reported recent decline in corruption in various public welfare programmes that pre-dated Aadhaar. For instance, in Chhattisgarh, PDS leakages declined from 51% in 2004-05 to around 9.3% in 2011-12 [See **Jean Dreze and Reetika Khera, *Understanding Leakages in PDS*, 50(7) EPW 39 at (2015) @pg 558, Vol. VI**]. Similarly, Bihar PDS leakage rates reduced from 90% in 2004 to around 24%, before ABBA was introduced [**Jean Dreze *et al*, *Food Security: Bihar on the Move*, 50(34) EPW 44 (2015)@ 562-63, Vol. VI]**

95. Thus, the State's own records show that the contribution of ABBA to plugging leakages is relatively minor, if at all. The State has failed to demonstrate that increased savings and better targeting are of an order of magnitude that justifies aforesaid serious rights' infringements. It is submitted that a simple balancing exercise – by citing purported savings against the cost of violation of fundamental rights – without a rigorous proportionality analysis, is not appropriate in the present case. [See ***Selvi*, ¶260 @ 571, Vol. II** that, considering the implications for "the whole population and future generations", *no* citizen could be forcibly subject to narco-analysis, even if it meant that some "hardened criminals" would benefit.]

96. Similarly, incorrect averments have been made in the context of LPG savings, using Aadhaar-enabled Direct Benefit Transfer ('**DBT**') scheme known as PAHAL which was

---

[34] See **Reply dated 02.08.2016 to Unstarred Qs No. [2730] in the Lok Sabha @pg 571, Vol. VI**

[35] E.g. Even though Assam had 0% Aadhaar seeding, as on 28.03.2017, 72,746 ration cards were deleted in Assam, which can have no bearing with Aadhaar. See **Lok Sabha Starred Qs No. 93 dt. 22.11.2016 @pg 572-575, Vol. VI** and **Lok Sabha Unstarred Qs No. 4289 dt. 28.03.2017 @pg 576-578, Vol. VI** See also **affidavit** of **Reetika Khera, para 9(iii) @pg 34, Vol. II.**

[36] See **affidavit** of **Reetika Khera, paras 7 and 9(iv) @pg 33, 35, Vol. II**

[37] See (a) **Anumeha Yadav, "Can biometrics stop the theft of rations: No, shows Gujarat", *Scroll.in* (2016) @pg 515-521 Vol. VI;** (b) **Affidavit** of **Reetika Khera, para 4(g) @pg 29, Vol. VI** and (c) para **6-11 of affidavit by Nikhil Dey dt. 21.04.16** in **W.P. No. 833/13**.

launched in 2014-15. The UIDAI, in their **Counter Affidavit dated 06.06.2017**, **pg 37-38**, stated that the de-duplication of beneficiaries using Aadhaar had resulted in huge savings to the tune of 14,672 crores (2014-15), 6,912 crores (2015-16) and 4,9824 crores (2016-17). *First*, the minutes of the Committee of Secretaries under the Chairmanship of Cabinet Secretary dated 30.11.2015 claimed that the de-duplication of beneficiaries using Aadhaar Number was able to identify only 9 lakh duplicate connections, and the total savings in the annual subsidy was only 91 crores [See **Addl. Affidavit dt 05.01.2018 in W.P.(C) No. 342/2017 @pg. 45-51, Vol. I]**. *Second*, the oil marketing companies in June 2012 (before the DBT scheme) conducted a de-duplication exercise with the assistance of National Informatics Centre using two parameters, viz., name and address. As a result, large number of duplicate connections were weeded out before the launch of PAHAL scheme. In fact, the CAG Report of 2015-16 pertaining to '*Implementation of PAHAL (DBTL) Scheme*' affirmed that the "the entire blocking of fake/duplicate or inactive consumers cannot be attributed to the outcome of PAHAL (DBTL) Scheme." [See **Addl. Affidavit dt 05.01.2018 in W.P.(C) No. 342/2017 @pg. 517, Vol. II]** *Third*, the huge savings in LPG subsidy is not even remotely attributable to Aadhaar Number. The CAG Report categorically stated that the burden of subsidies was comparably less for 2015-16 due to sharp decline in crude oil prices and reduction of consumers for subsidised cylinders due to #GiveItUP campaign and other DBT. [*See* **Addl. Affidavit dt 05.01.2018 in W.P.(C) No. 342/2017 @pg. 521, Vol. III**]

(c) Failure to consider less-invasive & effective alternate identification methods

97. It is the State's burden to show that Aadhaar is *both* necessary and proportionate, i.e. there exist no other alternatives that could have achieved their stated goals, using a less intrusive method [See ***Peck v UK,* (2003) ECHR 44, ¶¶76-87** and ***Modern Dental College & Research Centre v State of MP*, (2016) 7 SCC 353, ¶¶60-65]**. As a matter of fact, there exist less-invasive alternatives such as Smart Cards and social audits that have been included in sec. 12 of the NFSA and can help reduce diversion/leakages. In fact, these Smart Cards (using hologram, RFID chip, or OTP) have helped eliminate barriers of distance or location to avail entitlements, such as in Chhattisgarh.[38] Other alternatives such as food coupons, digitisation of records, doorstep delivery, SMS alerts, social audits, and toll-free helplines have also helped.[39] For instance, the Tamil Nadu PDS system is run using smart cards and electronic POS Machines and is in the process of replacing its 1.89 crore ration cards with smart cards, at a cost of over Rs 300 crores.[40] The very fact that the State has not examined such alternatives itself is enough to show that they have not discharged their burden under Art. 21. The fact that alternatives exist, and that the stated

---

[38] See **Payoj Jain *et al*, "Chhattisgarh's food ATMs: Portable benefits minus biometrics", *IndiaTogether*, 15th September 2014**

[39] See **Jean Dreze (supra) @pg 505, Vol. VI; Jean Dreze (supra) @pg 559, Vol. VI**

[40] See **PTI, 'Tamil Nadu to go Digital, Smart Cards replacing Ration Cards', ET @pg 582, Vol. VI**

purposes can be achieved without invading privacy, further fortifies the submissions of the Petitioners herein.

98. In fact, UK repealed the Identity Cards Act, 2006 through the **Identity Documents Act 2010**. Pertinently, documents that are considered inadequate for identity verification such as driving license are still considered adequate for the PoI process for Aadhaar.

99. The multiple cases of failures, as well as misuse and siphoning off of PDS money *through* Aadhaar, suggests that the issue is not so much whether the possibility of *abuse* can be a ground to strike down a legal provision, but whether the demonstrable inability to *use* and access the Aadhaar system in an effective fashion can ever satisfy the proportionality standard, and the departure from earlier, less intrusive legal measures.

100. In questions of infringement of fundamental rights, Courts have to decide on the proportionality of an imposition with greater scrutiny, when the primary decision maker (i.e. the State and UIDAI) did not give due weight to the competing balancing rights at stake [See ***Belfast City Council v Miss Behavin' Ltd,* (2007) UKHL 19, ¶ 37, 46**]. In the present case, the Aadhaar Act was drafted without considering privacy to be a fundamental right, worthy of constitutional protection.[41] In fact, it was the Union's expressly stated position that privacy was not part of Art. 21. Thus, the UID Scheme and subsequent Act did not consider the mandatory parting of identity information by residents as a violation of their bodily/decisional/informational privacy and as a form of compulsion, prohibited under Art. 21. In fact, even the stand of the Union in its multiple counter affidavits, and the studies annexed thereto, do not attempt any proportionality, or even balancing exercise. In light of this, it is submitted that the Act is unconstitutional.

March 13, 2018

K.V. Viswanathan
Senior Advocate

ASSISTED BY:

Vrinda Bhandari, Advocate
Gautam Bhatia, Advocate
N. Sai Vinod, Advocate

[41] See the views of the Government, as recorded in ***Puttaswamy*, ¶¶ 272, 331.4, 434-435.**