REPORTABLE

IN THE SUPREME COURT OF INDIA
CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO 494 OF 2012

JUSTICE K S PUTTASWAMY (RETD) & ANR ...PETITIONERS

Versus

UNION OF INDIA & ORS ...RESPONDENTS

WITH

T C (C) NO 151 OF 2013

T C (C) NO 152 OF 2013

W P (C) NO 833 OF 2013

W P (C) NO 829 OF 2013

T P (C) NO 1797 OF 2013

W P (C) NO 932 OF 2013

T P (C) NO 1796 OF 2013

CONMT. PET. (C) NO 144 OF 2014

T P (C) NO 313 OF 2014

T P (C) NO 312 OF 2014

SLP (CRL) NO 2524 OF 2014

W P (C) NO 37 OF 2015

W P (C) NO 220 OF 2015

CONMT. PET. (C) NO 674 OF 2015 in W P (C) NO 829 OF 2013

T P (C) NO 921 OF 2015

CONMT. PET. (C) NO 470 OF 2015

W P (C) NO 231 OF 2016

CONMT. PET. (C) NO 444 OF 2016

CONMT. PET. (C) NO 608 OF 2016

W P (C) NO 797 OF 2016

CONMT. PET. (C) NO 844 OF 2017

W P (C) NO 342 OF 2017

W P (C) NO 372 OF 2017

W P (C) NO 841 OF 2017

W P (C) NO 1058 OF 2017

W P (C) NO 966 OF 2017

W P (C) NO 1014 OF 2017

W P (C) NO 1002 OF 2017

W P (C) NO 1056 OF 2017

AND

WITH

CONMT. PET. (C) NO 34 OF 2018 in W P (C) NO 1014 OF 2017

J U D G M E N T

INDEX

[1] (2017) 10 SCC 1

F.4 Privacy Concerns in the Aadhaar Act

1. Consent during enrolment and authentication & the right to access information under the Aadhaar Act
2. Extent of information disclosed during authentication & sharing of core biometric information
3. Expansive scope of biometric information
4. Other concerns regarding the Aadhaar Act: Misconceptions regarding the efficacy of biometric information
5. No access to biometric records in database
6. Biometric locking
7. Key takeaways

G Legitimate state aim

G.I Directive Principles

G.2 Development and freedom

G.3 Identity and Identification

H Proportionality

H.I Harmonising conflicting rights

H.2 Proportionality standard in Indian jurisprudence

H.3 Comparative jurisprudence

H.4 Aadhaar: The proportionality analysis

H.5 Dignity and financial exclusion

H.6 Constitutional validity of Section 139AA of the Income Tax Act 1961

H.7 Linking of SIM cards and Aadhaar numbers

I Money laundering rules

J Savings in Section 59

K Rule of law and violation of interim orders

L Conclusion

Dr Dhananjaya Y Chandrachud, J

A Introduction: technology, governance and freedom

1 Technology and biometrics are recent entrants to litigation. Individually, each presents specific claims: of technology as the great enabler; and of biometrics as the unique identifier. As recombinant elements, they create as it were, new genetic material. Combined together, they present unforeseen challenges for governance in a digital age. Part of the reason for these challenges is that our law evolved in a radically different age and time. The law evolved instruments of governance in incremental stages. They were suited to the social, political and economic context of the time. The forms of expression which the law codified were developed when paper was ubiquitous. The limits of paper allowed for a certain freedom: the freedom of individuality and the liberty of being obscure. Governance with paper could lapse into governance on paper. Technology has become a universal language which straddles culture and language. It confronts institutions of governance with new problems. Many of them have no ready answers.

2 Technology questions the assumptions which underlie our processes of reasoning. It reshapes the dialogue between citizens and the state. Above all, it tests the limits of the doctrines which democracies have evolved as a shield which preserves the sanctity of the individual.

3 In understanding the interface between governance, technology and freedom, this case will set the course for the future. Our decision must address the dialogue between technology and power. The decision will analyse the extent to which technology has reconfigured the role of the state and has the potential to reset the lines which mark off no-fly zones: areas where the sanctity of the individual is inviolable. Our path will define our commitment to limited government. Technology confronts the future of freedom itself.

4 Granville Austin, the eminent scholar of the Indian Constitution had prescient comments on the philosophy of the Indian Constitution. He found it in three strands:

> "The Constitution…may be summarized as having three strands: protecting and enhancing national unity and integrity; establishing the institutions and spirit of democracy; and fostering a social revolution to better the mass of Indians...the three strands are mutually dependent and inextricably intertwined. Social revolution could not be sought or gained at the expense of democracy. Nor could India be truly democratic unless the social revolution had to establish a just society. Without national unity, democracy would be endangered and there would be little progress toward social and economic reform. And without democracy and reform, the nation would not hold together. With these three strands, the framers had spun a seamless web. Undue strain on, or slackness in any one strand would distort the web and risk its destruction and, with it, the destruction of the nation. Maintaining harmony between the strands predictably would present those who later work the Constitution with great difficulties…"[2]

[2] Granville Austin, Working a Democratic Constitution: A History of the Indian Experience, Oxford University Press (2003) at page 6

These three strands are much like the polycentric web of which Lon Fuller has spoken.[3] A pull on one strand shakes the balance between the others. The equilibrium between them preserves the equilibrium of the Constitution.

5 This Court has been tasked with adjudicating on the constitutional validity of the Aadhaar project. The difficulties that Granville Austin had predicted would arise in harmonising the strands of the "seamless web" are manifested in the present case. This case speaks to the need to harmonise the commitment to social welfare while safeguarding the fundamental values of a liberal constitutional democracy.

6 To usher in a social revolution, India espoused the framework of a welfare state. The Directive Principles are its allies. The state is mandated to promote the welfare of its citizens by securing and protecting as effectively as possible a social order in which there is social, economic and political justice. Government plays a vital role in the social and economic upliftment of the nation's citizenry by espousing equitable distribution of resources and creating equal opportunities. These are ideals that are meant to guide and govern State action. The State's commitment to improve welfare is manifested through the measures and programmes which it pursues.

[3] Lon L. Fuller and Kenneth I. Winston, The Forms and Limits of Adjudication, Harvard Law Review, Vol. 92, (1978), at pages 353-409

7 The Constitution of India incorporated a charter of human freedoms in Part III and a vision of transformative governance in Part IV. Through its rights jurisprudence, this Court has attempted to safeguard the rights in Part III and to impart enforceability to at least some of the Part IV rights by reading them into the former, as intrinsic to a constitutionally protected right to dignity. The Directive Principles are a reminder of the positive duties which the state has to its citizens. While social welfare is a foundational value, the Constitution is the protector of fundamental human rights. In subserving both those ideals, it has weaved a liberal political order where individual rights and freedoms are at the heart of a democratic society. The Constitution seeks to fulfil its liberal values by protecting equality, dignity, privacy, autonomy, expression and other freedoms.

8 Two recent books have explored the complexities of human identity. In "The Lies That Bind: Rethinking Identity"[4], Kwame Anthony Appiah states that a liberal constitutional democracy is not a fate but a project. He draws inspiration from the Roman playwright Terence who observes: "I am human. I think nothing human alien to me." Francis Fukuyama, on the other hand has a distinct nuance about identity. In "Identity: The Demand for Dignity and the Politics of Enlightenment[5], he writes about how nations can facilitate "integrative national identities" based on liberal democratic values. Reviewing the books, Anand Giridharadas noted that Fukuyama's sense of identity is

[4] Kwame Anthony Appiah**,** The Lies That Bind: Rethinking Identity, Liveright Publishing (2018).
[5] Francis Fukuyama, Identity: The Demand for Dignity and the Politics of Enlightenment, Farrar, Straus and Giroux (2018).

"large enough to be inclusive but small enough to give people a real sense of agency over their society."[6]. Appiah and Fukuyama present two variants – for Appiah it has a cosmopolitan and global nature while it is more integrated with a nation state, for Fukuyama, though firmly rooted in a liberal constitutional order.

9 India has participated in and benefited from the reconfiguring of technology by the global community. We live in an age of information and are witness to a technological revolution that pervades almost every aspect of our lives. Redundancies and obsolescence are as ubiquitous as technology itself. Technology is a great enabler. Technology can be harnessed by the State in furthering access to justice and fostering good governance.

10 In an age symbolised by an information revolution, society is witnessing a shift to a knowledge economy[7]. In a knowledge economy, growth is dependent on the 'quantity, quality, and accessibility'[8] of information. The quest for digital India must nonetheless be cognisant of the digital divide. Access confronts serious impediments. Large swathes of the population have little or no access to the internet or to the resources required for access to information. With the growth of the knowledge economy, our constitutional jurisprudence has expanded privacy rights. A digital nation must not submerge

[6] Anand Giridharadas, 'What is Identity?', The New York Times, 27 August, 2018.
[7] Peter F Drucker, The Age of Discontinuity: Guidelines to Our Changing Society, Harper & Row (1969). Drucker's book popularized the term 'Knowledge Economy'.
[8] 'What is Knowledge Economy?', IGI Global: Disseminator of Knowledge, available at: https://www.igi-global.com/dictionary/indigenous-knowledges-and-knowledge-codification-in-the-knowledge-economy/16327

the identities of a digitised citizen. While data is the new oil, it still eludes the life of the average citizen. If access to welfare entitlements is tagged to unique data sets, skewed access to informational resources should not lead to perpetuating the pre-existing inequalities of access to public resources. An identification project that involves the collection of the biometric and demographic information of 1.3 billion people[9], creating the largest biometric identity project in the world, must be scrutinized carefully to assess its compliance with human rights.

11 Empowered by the technology that accompanied the advent of the information age, the Aadhaar project was envisioned and born. The project is a centralised nation-wide identification system based on biometric technology. It aims to be a game changer in the delivery of welfare benefits through the use of technology. The project seeks to facilitate de-duplication, prevent revenue leakages and ensure a more cost and time efficient procedure for identification. Conceptualised on the use of biometrics and authentication, the Aadhaar identity card was originally introduced as a matter of voluntary choice. It was made a requirement for state subsidies and benefits for which, expenses are incurred from the Consolidated Fund of India. It was later expanded to become necessary to avail of a host of other services. The project is multifaceted and expansive. Perhaps no similar national identity program exists in the world. The Aadhaar project has multifarious aspects, all

[9] Krishnadas Rajagopal, 'Aadhaar in numbers: key figures from UIDAI CEO's presentation to the Supreme Court', The Hindu, (March 22, 2018). Aadhaar enrollment as of March 2018 stood at over 1 billion.

of which have been the subject of a detailed challenge by the Petitioners. They have been met with an equally strong defence from the government, which has argued that the programme is indispensable to curb corruption, fraud and black money.

12 The Aadhaar project raises two crucial questions: First, are there competing interests between human rights and 'welfare furthering technology' in democratic societies? Can technologies which are held out to bring opportunities for growth, also violate fundamental human freedoms? Second, if the answer to the first is in the affirmative, how should the balance be struck between these competing interests?

13 Efficiency is a significant facet of institutional governance. But efficiencies can compromise dignity. When efficiency becomes a universal mantra to steam-roll fundamental freedoms, there is a danger of a society crossing the line which divides democracy from authoritarian cultures. At the heart of the grounds on which the Aadhaar project has been challenged, lies the issue of power. Our Constitution is a transformative document in many ways. One of them is in defining and limiting the State's powers, while expanding the ambit of individual rights and liberties. It protects citizens from totalitarian excesses and establishes order between the organs of the State, between the State and citizens and between citizens. Most importantly, it reaffirms the position of the individual as the core defining element of the

polity. That is the justification to restrain power by empowering all citizens to be authors of their destiny. According to the Petitioners, the technological potential as well as the actual implementation of the Aadhaar project alters the balance between the state and its citizens in this relational sphere and has the potential to permanently redistribute power within the constitutional framework.

14 As far as citizen-state relations are concerned, the Constitution was framed to balance the rights of the individual against legitimate State interests. Being transformative, it has to be interpreted to meet the needs of a changing society. As the interpreter of the Constitution, it is the duty of this Court to be vigilant against State action that threatens to upset the fine balance between the power of the state and rights of citizens and to safeguard the liberties that inhere in our citizens.

15 The present case involves issues that travel to the heart of our constitutional structure as a democracy governed by the rule of law. Among them is the scope of this Court's power of judicial review. The Aadhaar legislation was passed as a money bill in the Lok Sabha. Whether it was permissible, in constitutional terms, to by-pass the Rajya Sabha, is the question. The role of the Rajya Sabha in a bicameral legislative structure, the limits of executive power when it affects fundamental rights and the duty of the

state to abide by interim orders of this Court are matters which will fall for analysis in the case.

16 The case is hence as much about the rule of law and institutional governance. Accountability is a key facet of the rule of law. Professor Upendra Baxi has remarked:

> "The problem of human rights, in situations of mass poverty, is thus one of redistribution, access and needs. In other words, it is a problem of "development", a process of planned social change through continuing exercise of public power. As there is no assurance that public power will always, or even in most cases, be exercised in favour of the deprived and dispossessed, an important conception of development itself is accountability, by the wielders of public power, to the people affected by it and people at large. Accountability is the medium through which we can strike and maintain a balance between the governors and the governed."[10]

These are some of the unique challenges of this case. They must be analysed in the context of our constitutional framework. The all-encompassing nature of the Aadhaar project, its magnitude and the resultant impact on citizens' fundamental rights, make it imperative to closely scrutinize the structure and effect of the project. For this will determine the future of freedom.

[10] Upendra Baxi, The Right To Be Human: Some Heresies, India International Centre Quarterly, Vol. 13, (1986).

B The Puttaswamy[11] principles

17 A unanimous verdict by a nine judge Bench declared privacy to be constitutionally protected, as a facet of liberty, dignity and individual autonomy. In a voluminous judgment, the Court traced the origins of privacy and its content. The decision lays down the test of proportionality to evaluate the constitutional validity of restrictions on the right to privacy.

18 The protection of privacy emerges both from its status as a natural right inhering in every individual as well as its position as "a constitutionally protected right". As a constitutional protection, privacy traces itself to the guarantee of life and personal liberty in Article 21 of the Constitution as well as to other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III.

B.I Origins: privacy as a natural right

19 **Puttaswamy** holds that the right to privacy inheres in every individual as a natural right. It is inalienable and attaches to every individual as a pre-condition for being able to exercise their freedom. The judgment of four judges (with which Justice Sanjay Kishan Kaul concurred) held :

> "42. Privacy is a concomitant of the right of the individual to exercise control over his or her personality. **It finds an origin**

[11] Justice K S Puttaswamy (Retd) v Union of India ("Puttaswamy"), (2017) 10 SCC 1

> **in the notion that there are certain rights which are natural to or inherent in a human being**. Natural rights are inalienable because they are inseparable from the human personality."[12] (Emphasis supplied)
>
> "319. **Life and personal liberty are not creations of the Constitution. These rights are recognised by the Constitution as inhering in each individual as an intrinsic and inseparable part of the human element which dwells within**."[13] (Emphasis supplied)

In his concurring opinion, S A Bobde, J. opined:

> "392…Privacy, with which we are here concerned, **eminently qualifies as an inalienable natural right,** intimately connected to two values whose protection is a matter of universal moral agreement: the innate dignity and autonomy of man."[14] (Emphasis supplied)

Similarly, in his concurring opinion, Nariman, J. opined:

> "532…It was, therefore, argued before us that given the international conventions referred to hereinabove and the fact that this right inheres in every individual by virtue of his being a human being, such right is not conferred by the Constitution but is only recognized and given the status of being fundamental. **There is no doubt that the petitioners are correct in this submission.**"[15]
> (Emphasis supplied)

In his concurring opinion, Abhay Manohar Sapre, J. opined:

> "557. In my considered opinion, **"right to privacy of any individual" is essentially a natural right, which inheres in every human being by birth…It is indeed inseparable and inalienable from human being**."[16]
> (Emphasis supplied)

[12] Ibid, at page 365
[13] Ibid, at page 508
[14] Ibid, at pages 536-537
[15] Ibid, at page 605
[16] Ibid, at page 614

The judgment authoritatively settles the position. While privacy is recognized and protected by the Constitution as an intrinsic and inseparable part of life, liberty and dignity, it inheres in every individual as a natural right.

B.2 Privacy as a constitutionally protected right : liberty and dignity

20 The judgment placed the individual at the centre of the constitutional rights regime. The individual lies at the core of constitutional focus. The ideals of justice, liberty, equality and fraternity animate the vision of securing a dignified existence to the individual. The Court held that privacy attaches to the person and not the place where it is associated. Holding that privacy protects the autonomy of the individual and the right to make choices, the judgment of four judges held:

> "108….**The individual is the focal point of the Constitution because it is in the realisation of individual rights that the collective well being of the community is determined**. Human dignity is an integral part of the Constitution.[17]
>
> "266. **Our Constitution places the individual at the forefront of its focus, guaranteeing civil and political rights in Part III and embodying an aspiration for achieving socio-economic rights in Part IV**."
> (Emphasis supplied)

It was held that privacy rests in every individual "irrespective of social class or economic status" and that every person is entitled to the intimacy and autonomy that privacy protects:

[17] Ibid, at page 403

> "271...It is privacy as an intrinsic and core feature of life and personal liberty which enables an individual to stand up against a programme of forced sterilization. Then again, it is privacy which is a powerful guarantee if the State were to introduce compulsory drug trials of non-consenting men or women. **The sanctity of marriage, the liberty of procreation, the choice of a family life and the dignity of being are matters which concern every individual irrespective of social strata or economic well being. The pursuit of happiness is founded upon autonomy and dignity. Both are essential attributes of privacy which makes no distinction between the birth marks of individuals.**"[18] (Emphasis supplied)

21 Recognizing that civil-political rights are not subservient to socio-economic rights, the Court held that "conditions necessary for realizing or fulfilling socio-economic rights do not postulate the subversion of political freedom."

> "266...The refrain that the poor need no civil and political rights and are concerned only with economic well-being has been utilised through history to wreak the most egregious violations of human rights. Above all, it must be realised that it is the right to question, the right to scrutinize and the right to dissent which enables an informed citizenry to scrutinize the actions of government. Those who are governed are entitled to question those who govern, about the discharge of their constitutional duties including in the provision of socio-economic welfare benefits. The power to scrutinize and to reason enables the citizens of a democratic polity to make informed decisions on basic issues which govern their rights.[19]
>
> 267... Conditions of freedom and a vibrant assertion of civil and political rights promote a constant review of the justness of socio-economic programmes and of their effectiveness in addressing deprivation and want. Scrutiny of public affairs is founded upon the existence of freedom. Hence civil and political rights and socio-economic rights are complementary and not mutually exclusive."[20]

[18] Ibid, at page 484
[19] Ibid, at pages 481-482
[20] Ibid, at page 482

Significantly, the Court rejected the submission that there is a conflict between civil-political rights and socio-economic rights. Both in the view of the Court are an integral part of the constitutional vision of justice.

22 Privacy, it was held, reflects the right of the individual to exercise control over his or her personality. This makes privacy the heart of human dignity and liberty. Liberty and dignity are complementary constitutional entities. Privacy was held to be integral to liberty. Privacy facilitates the realization of constitutional freedoms. This Court held thus:

> "119. To live is to live with dignity. The draftsmen of the Constitution defined their vision of the society in which constitutional values would be attained by emphasising, among other freedoms, liberty and dignity. So fundamental is dignity that it permeates the core of the rights guaranteed to the individual by Part III. Dignity is the core which unites the fundamental rights because the fundamental rights seek to achieve for each individual the dignity of existence. Privacy with its attendant values assures dignity to the individual and it is only when life can be enjoyed with dignity can liberty be of true substance. Privacy ensures the fulfilment of dignity and is a core value which the protection of life and liberty is intended to achieve."[21]
>
> 127...The right to privacy is an element of human dignity. The sanctity of privacy lies in its functional relationship with dignity. Privacy ensures that a human being can lead a life of dignity by securing the inner recesses of the human personality from unwanted intrusion. Privacy recognises the autonomy of the individual and the right of every person to make essential choices which affect the course of life. In doing so privacy recognises that living a life of dignity is essential for a human being to fulfil the liberties and freedoms which are the cornerstone of the Constitution."[22]

[21] Ibid, at pages 406-407
[22] Ibid, at page 413

23 The assurance of human dignity enhances the quality of life. The "functional relationship" between privacy and dignity secures the "inner recesses of the human personality from unwanted intrusion". Privacy by recognizing the autonomy of an individual, protects the right to make choices essential to a dignified life. It thus enables the realization of constitutional liberties and freedoms. It was held in the judgment:

> "322. Privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. At a normative level privacy sub-serves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty.[23]
>
> 298…Dignity cannot exist without privacy. Both reside within the inalienable values of life, liberty and freedom which the Constitution has recognised. Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and protects for the individual a zone of choice and self-determination."[24]

24 Privacy is founded on the autonomy of the individual. The ability to make choices is at the core of the human personality. Its inviolable nature is manifested in the ability to make intimate decisions about oneself with a legitimate expectation of privacy. Privacy guarantees constitutional protection to all aspects of personhood. Privacy was held to be an "essential condition" for the exercise of most freedoms. As such, given that privacy and liberty are intertwined, privacy is necessary for the exercise of liberty. Bobde J, in his separate opinion held that:

[23] Ibid, at page 508
[24] Ibid, at page 499

> "409...Liberty and privacy are integrally connected in a way that privacy is often the basic condition necessary for exercise of the right of personal liberty. There are innumerable activities which are virtually incapable of being performed at all and in many cases with dignity unless an individual is left alone or is otherwise empowered to ensure his or her privacy.[25]
>
> 411... Both dignity and privacy are intimately intertwined and are natural conditions for the birth and death of individuals, and for many significant events in life between these events. Necessarily, then, the right of privacy is an integral part of both 'life' and 'personal liberty' under Article 21, and is intended to enable the rights bearer to develop her potential to the fullest extent made possible only in consonance with the constitutional values expressed in the Preamble as well as across Part III."[26]

25 Apart from being a natural law right, the right to privacy was held to be a constitutionally protected right flowing from Article 21. Privacy is an indispensable element of the right to life and personal liberty under Article 21 and as a constitutional value which is embodied in the fundamental freedoms embedded in Part III of the Constitution. Tracing out the course of precedent in Indian jurisprudence over the last four decades, the view of four judges holds:

> "103. The right to privacy has been traced in the decisions which have been rendered over more than four decades to the guarantee of life and personal liberty in Article 21 and the freedoms set out in Article 19."[27]
>
> "320. Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution…"[28]

[25] Ibid, at page 543
[26] Ibid, at page 544
[27] Ibid, at page 401
[28] Ibid, at page 508

In a similar vein, Chelameswar J. while concurring with the view of four judges held:

> "375. The right to privacy is certainly one of the core freedoms which is to be defended. It is part of liberty within the meaning of that expression in Article 21."[29]

26 Being indispensable to dignity and liberty, and essential to the exercise of freedoms aimed at the self-realization of every individual, privacy was held to be a common theme running across the freedoms and rights guaranteed not just by Article 21, but all of Part III of the Constitution. Bobde J. in his separate opinion held that:

> "406. It is not possible to truncate or isolate the basic freedom to do an activity in seclusion from the freedom to do the activity itself. The right to claim a basic condition like privacy in which guaranteed fundamental rights can be exercised must itself be regarded as a fundamental right. **Privacy, thus, constitutes the basic, irreducible condition necessary for the exercise of 'personal liberty' and freedoms guaranteed by the Constitution. It is the inarticulate major premise in Part III of the Constitution.**[30]
>
> 415. **Privacy is the necessary condition precedent to the enjoyment of any of the guarantees in Part III. As a result, when it is claimed by rights bearers before constitutional courts, a right to privacy may be situated not only in Article 21, but also simultaneously in any of the other guarantees in Part III.** In the current state of things, Articles 19(1), 20(3), 25, 28 and 29 are all rights helped up and made meaningful by the exercise of privacy."
> (Emphasis supplied)

[29] Ibid, at page 531
[30] Ibid, at pages 541-542

B.3 Contours of privacy

27 Privacy has been held to have distinct connotations including (i) spatial control; (ii) decisional autonomy; and (iii) informational control. The judgment of four judges held that:

> "248. Spatial control denotes the creation of private spaces. Decisional autonomy comprehends intimate personal choices such as those governing reproduction as well as choices expressed in public such as faith or modes of dress. Informational control empowers the individual to use privacy as a shield to retain personal control over information pertaining to the person."

Similarly, Nariman J. in his separate opinion held:

> "521. In the Indian context, a fundamental right to privacy would cover at least the following three aspects:
> - Privacy that involves the person i.e. when there is some invasion by the State of a person's rights relatable to his physical body, such as the right to move freely;
> - Informational privacy which does not deal with a person's body but deals with a person's mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him. Unauthorised use of such information may, therefore lead to infringement of this right; and
> - The privacy of choice, which protects an individual's autonomy over fundamental personal choices."[31]

28 However, it was held that this is not an exhaustive formulation of entitlements. In recording its conclusions, the opinion of four judges held:

> **"**324. **This Court has not embarked upon an exhaustive enumeration or a catalogue of entitlements or interests comprised in the right to privacy. The Constitution must evolve with the felt necessities of time to meet the challenges thrown up in a democratic order governed by the rule of law.** The meaning of the Constitution cannot be

[31] Ibid, at page 598

> frozen on the perspectives present when it was adopted. Technological change has given rise to concerns which were not present seven decades ago and the rapid growth of technology may render obsolescent many notions of the present. **Hence the interpretation of the Constitution must be resilient and flexible to allow future generations to adapt its content bearing in mind its basic or essential features.**"[32] (Emphasis supplied)

Additionally, Bobde J., in his separate opinion held that the right to privacy may also inhere in other parts of the Constitution beyond those specified in the judgment:

> "415. Therefore, privacy is the necessary condition precedent to the enjoyment of any of the guarantees in Part III. As a result, when it is claimed by rights bearers before constitutional courts, a right to privacy may be situated not only in Article 21, but also simultaneously in any of the other guarantees in Part III. In the current state of things, Articles 19(1), 20(3), 25, 28 and 29 are all rights helped up and made meaningful by the exercise of privacy. **This is not an exhaustive list. Future developments in technology and social ordering may well reveal that there are yet more constitutional sites in which a privacy right inheres that are not at present evident to us.**"[33] (Emphasis supplied)

B.4 Informational privacy

29 **Puttaswamy** held that informational privacy is an essential aspect of the fundamental right to privacy. It protects an individual's free, personal conception of the 'self.' Justice Nariman held that informational privacy "deals with a person's mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him". Any unauthorised use of such information may therefore lead to infringement of the

[32] Ibid, at page 509
[33] Ibid, at page 545

right to privacy. In his concurring judgment, Justice Kaul held that informational privacy provides the right to an individual "to disseminate certain personal information for limited purposes alone". Kaul J. in his separate opinion held:

> "620…**The boundaries that people establish from others in society are not only physical but also informational.** There are different kinds of boundaries in respect to different relations. Privacy assists in preventing awkward social situations and reducing social frictions. Most of the information about individuals can fall under the phrase "none of your business". … An individual has the right to control one's life while submitting personal data for various facilities and services. **It is but essential that the individual knows as to what the data is being used for with the ability to correct and amend it. The hallmark of freedom in a democracy is having the autonomy and control over our lives which becomes impossible, if important decisions are made in secret without our awareness or participation**."[34] (Emphasis supplied)

30 A reasonable expectation of privacy requires that data collection does not violate the autonomy of an individual. The judgment of four judges noted the centrality of consent in a data protection regime. This was also highlighted in the separate concurring opinion of Justice Kaul:

> "625. Every individual should have a right to be able to exercise control over his/her own life and image as portrayed to the world and to control commercial use of his/her identity. This also means that an individual may be permitted to prevent others from using his image, name and other aspects of his/her personal life and identity for commercial purposes without his/her consent."[35]

[34] Ibid, at page 627
[35] Ibid, at page 629

Consent, transparency and control over information are crucial to informational privacy. In this structure, Court has principally focused on the "individual" as central to our jurisprudence.

B.5 Restricting the right to privacy

31 There is an inherent importance of giving a constitutional status to privacy. Justice Nariman dealt with this:

> "490...The recognition of such right in the fundamental rights chapter of the Constitution is only a recognition that such right exists notwithstanding the shifting sands of majority governments. Statutes may protect fundamental rights; they may also infringe them. In case any existing statute or any statute to be made in the future is an infringement of the inalienable right to privacy, this Court would then be required to test such statute against such fundamental right and if it is found that there is an infringement of such right, without any countervailing societal or public interest, it would be the duty of this Court to declare such legislation to be void as offending the fundamental right to privacy."[36]

A constitutional right may embody positive and negative 'aspects'. They signify mandates. At an affirmative level, they emphasise the content and diversity of our liberties. As a 'negative', they impose restraints on the state and limit the power of the state to intrude upon the area of personal freedom. 'Negative' in this sense reflects a restraint: the fundamental rights are a restraining influence on the authority of power. In addition to keeping itself within the bounds of its authority, the state may have a positive obligation to perform. Rights such as informational privacy and data protection mandate

[36] Ibid, at pages 580-581

that the state must bring into being a viable legal regime which recognizes, respects, protects and enforces informational privacy. Informational privacy requires the state to protect it by adopting positive steps to safeguard its cluster of entitlements. The right to informational privacy is not only vertical (asserted and protected against state actors) but horizontal as well. Informational privacy requires legal protection because the individual cannot be left to an unregulated market place. Access to and exploitation of individual personal data – whether by state or non-state entities – must be governed by a legal regime built around the principles of consent, transparency and individual control over data at all times.

32 Privacy, being an intrinsic component of the right to life and personal liberty, it was held that the limitations which operate on those rights, under Article 21, would operate on the right to privacy. Any restriction on the right to privacy would therefore be subjected to strict constitutional scrutiny. The constitutional requirements for testing the validity of any encroachment on privacy were dealt with in the judgment as follows:

> "325… In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them."[37]

[37] Ibid, at page 509

These three-fold requirements emerge from the procedural and content-based mandate of Article 21. The first requirement is the enactment of a valid law, which justifies an encroachment on privacy. The second requirement of a legitimate State aim ensures that the law enacted to restrict privacy is constitutionally reasonable and does not suffer from **manifest arbitrariness**. The third requirement of proportionality ensures that the nature and quality of the encroachment on the right to privacy is not disproportionate to the purpose of the law. Proportionality requires the State to justify that the means which are adopted by the legislature would encroach upon the right to privacy only to the minimum degree necessary to achieve its legitimate interest.

Justice Nariman held thus:

> "495…Statutory provisions that deal with aspects of privacy would continue to be tested on the ground that they would violate the fundamental right to privacy, and would not be struck down, if it is found on a balancing test that the social or public interest and the reasonableness of the restrictions would outweigh the particular aspect of privacy claimed. If this is so, then statutes which would enable the State to contractually obtain information about persons would pass muster in given circumstances, provided they safeguard the individual right to privacy as well… in pursuance of a statutory requirement, if certain details need to be given for the concerned statutory purpose, then such details would certainly affect the right to privacy, but would on a balance, pass muster as the State action concerned has sufficient inbuilt safeguards to protect this right – viz. the fact that such information cannot be disseminated to anyone else, save on compelling grounds of public interest."[38]

33 While five judges of the Court adopted the "proportionality" standard to test a law infringing privacy, Justice Chelameswar discussed the need to

[38] Ibid, at page 583

apply of a "compelling state interest" standard, describing it as the "highest standard of scrutiny that a court can adopt". Describing Article 21 as the "bedrock" of privacy, the learned Judge held:

> "379…If the spirit of liberty permeates every claim of privacy, it is difficult if not impossible to imagine that any standard of limitation, other than the one under Article 21 applies.[39]
>
> 380. The just, fair and reasonable standard of review under Article 21 needs no elaboration. It has also most commonly been used in cases dealing with a privacy claim hitherto. Gobind resorted to the compelling state interest standard in addition to the Article 21 reasonableness enquiry. From the United States where the terminology of 'compelling state interest' originated, a strict standard of scrutiny comprises two things- a 'compelling state interest' and a requirement of 'narrow tailoring' (narrow tailoring means that the law must be narrowly framed to achieve the objective). As a term, compelling state interest does not have definite contours in the US. Hence, it is critical that this standard be adopted with some clarity as to when and in what types of privacy claims it is to be used. **Only in privacy claims which deserve the strictest scrutiny is the standard of compelling State interest to be used. As for others, the just, fair and reasonable standard under Article 21 will apply. When the compelling State interest standard is to be employed must depend upon the context of concrete cases**."[40] (Emphasis supplied)

Justice Chelameswar's view accepts the 'fair, just and reasonable' standard in the generality of cases, carving an exception in cases of a certain category where a heightened scrutiny must apply. Those categories of exception are not spelt out. They would, as the judge opined, be evolved on a case by case basis.

[39] Ibid, at page 532
[40] Ibid, at pages 532-533

34 The Bench of nine judges had held that the contours of privacy exist across the spectrum of constitutionally protected freedoms. Privacy was held to be a necessary condition precedent to the enjoyment of the guarantees in Part III. This has enhanced the scope of the protection guaranteed to privacy. Consequently, privacy infringements will generally have to satisfy the other tests applicable apart from those under Article 21. In his concurring opinion, Justice S A Bobde held:

> "427. Once it is established that privacy imbues every constitutional freedom with its efficacy and that it can be located in each of them, **it must follow that interference with it by the state must be tested against whichever one or more Part III guarantees whose enjoyment is curtailed.** As a result, privacy violations will usually have to answer to tests in addition to the one applicable to Article 21, Such a view would be wholly consistent with R. C. Cooper v. Union of India."[41] (Emphasis supplied)

Any attempt by the State to restrict privacy must therefore meet the constitutional requirements prescribed for each provision of Part III, which the restriction infringes. In his concurring opinion, Justice Nariman held thus:

> "488... Every State intrusion into privacy interests which deals with the physical body or the dissemination of information personal to an individual or personal choices relating to the individual would be **subjected to the balancing test prescribed under the fundamental right that it infringes depending upon where the privacy interest claimed is founded**."[42] (Emphasis supplied)

Justice Nariman further held:

> "526…**when it comes to restrictions on this right, the drill of various Articles to which the right relates must be scrupulously followed.** For example, if the restraint on privacy is over fundamental personal choices that an

[41] Ibid, at page 549
[42] Ibid, at page 580

> individual is to make, State action can be restrained under Article 21 read with Article 14 if it is arbitrary and unreasonable; and under Article 21 read with Article 19(1)(a) only if it relates to the subjects mentioned in Article 19(2) and the tests laid down by this Court for such legislation or subordinate legislation to pass muster under the said Article. Each of the tests evolved by this Court, qua legislation or executive action, under Article 21 read with Article 14; or Article 21 read with Article 19(1) (a) in the aforesaid examples must be met in order that State action must pass muster."[43] (Emphasis supplied)

The constitutional guarantee on protection of privacy was placed on a sure foundation. Since emanations of privacy are traceable to various rights guaranteed by Part III, a law or executive action which encroaches on privacy must meet the requirements of the constitutionally permissible restriction in relation to each of the fundamental rights where the claim is founded.

B.6 Legitimate state interests

35 Recognizing that the right to privacy is not absolute, the judgment recognizes that legitimate state interests may be a valid ground for the curtailment of the right subject to the tests laid down for the protection of rights. Justice Nariman held:

> "526...This right is subject to reasonable regulations made by the State to protect legitimate State interests or public interest. However, when it comes to restrictions on this right, the drill of various Articles to which the right relates must be scrupulously followed."[44]

[43] Ibid, at page 601
[44] Ibid, at page 601

Recognizing that a legitimate state aim is a pre-requisite for any restriction on the right, the judgment of four judges held:

> "310…the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness."

36 The judgment sets out illustrations of legitimate State interests. The provisos to various fundamental rights were held to be an obvious restriction on the right to privacy. It was held that the State does have a legitimate interest in collection and storage of private information when it is related to security of the nation. Apart from the concerns of national security, an important State interest, it was held, lies in ensuring that scarce public resources reach the beneficiaries for whom they are intended. It was held thus:

> "311...Allocation of resources for human development is coupled with a legitimate concern that the utilisation of resources should not be siphoned away for extraneous purposes… Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the state to insist on the collection of authentic data."[45]

Prevention and investigation of crime, protection of the revenue and public health were demarcated as being part of other legitimate aims of the State. The judgment places an obligation on the State to ensure that while its legitimate interests are duly preserved the data which the State collects is

[45] Ibid, at page 505

used only for the legitimate purposes of the State and is "not to be utilised unauthorizedly for extraneous purposes."

37 However, reiterating that every facet of privacy is to be protected, the judgment held that there should be a careful balance between individual interests and legitimate concerns of the state. Justice Nariman, in his separate opinion held:

> "488. Every State intrusion into privacy interests which deals with the physical body or the dissemination of information personal to an individual or personal choices relating to the individual would be subjected to the balancing test prescribed under the fundamental right that it infringes depending upon where the privacy interest claimed is founded."[46]

38 The judgment in **Puttaswamy** recognizes the right to privacy as a constitutional guarantee protected as intrinsic to the freedoms guaranteed by Part III of the Constitution. Privacy is integral to the realization of human dignity and liberty. A society which protects privacy, values the worth of individual self-realization. For it is in the abyss of solitude that the innermost recesses of the mind find solace to explore within and beyond.

[46] Ibid, at page 580

C Submissions

C.I Petitioners' submissions

The petitioners challenge the constitutional validity of:

a. The Aadhaar programme that operated between 28.01.2009 till the coming into force of the Aadhaar Act, 2016 on 12.07.2016;
b. The Aadhaar Act, 2016 (and alternatively certain provisions of the Act);
c. Regulations framed under the Aadhaar Act, 2016;
d. Elements of the Aadhaar programme that continue to operate without the cover of the Act;
e. Subordinate legislation including the Money Laundering (Amendment) Rules, 2017;
f. All notifications issued under Section 7 of the Aadhaar Act in so far as they make Aadhaar mandatory for availing of certain benefits, services and subsidies; and
g. Actions which made Aadhaar mandatory even where the activity is not covered by Section 7 of the Act.

Mr Shyam Divan, learned Senior Counsel submitted that the Aadhaar project and Act are ultra vires on the following grounds:

i The project and the Act violate the fundamental right to privacy;

ii The architecture of the Aadhaar project enables pervasive surveillance by the State;

iii The fundamental constitutional feature of a 'limited government' - which is the sovereignty of the people and limited government authority- is changed completely post Aadhaar and reverses the relationship between the citizen and the State;

iv Due to the unreliability of biometric technology, there are authentication failures which lead to the exclusion of individuals from welfare schemes;

v A citizen or resident in a democratic society has a choice to identify herself through different modes in the course of her interactions generally in society, as well as in her interactions with the State. Mandating identification by only one mode is highly intrusive, excessive and disproportionate and violates Articles 14, 19 and 21; and

vi The procedure adopted by the State before and after the enactment of the law is violative of Articles 14 and 21 because:

a. There is no informed consent at the time of enrolment;

b. UIDAI does not have control over the enrolling agencies and requesting entities that collect sensitive personal information which facilitates capture, storage and misuse of information; and

c. The data collected and uploaded into the CIDR is not verified by any government official designated by UIDAI.

Mr Kapil Sibal, learned Senior Counsel submits that the provisions of the Aadhaar Act are unconstitutional for the following reasons:

i The aggregation and concentration of sensitive personal information under the Aadhaar Act is impermissible because it is capable of being used to affect every aspect of an individual's personal, professional, religious and social life. It is therefore violative of the individual freedoms guaranteed under Articles 19(1)(a) to 19(1)(g), 21 and 25 of the Constitution;

ii Such aggregation of information is also an infringement of informational privacy, which has been recognised in **Puttaswamy**;

iii Making Aadhaar mandatory unreasonably deprives citizens of basic rights and entitlements and infringes Article 21 of the Constitution;

iv Use of Aadhaar as an exclusive identity for availing of subsidies, benefits and services is disproportionate and violates Article 14 for being arbitrary and discriminatory against persons otherwise entitled to such benefits;

v Collection and storage of data with the government under the Aadhaar Act is violative of the right to protection from self-incrimination, and the right to

privacy and personal dignity and bodily Integrity envisaged under Article 20(3) and Article 21 of the Constitution;

vi To prescribe that Aadhaar is the only identity that enables a person to receive entitlements is contrary to the right of an individual under the Constitution to identify the person through other prescribed documentation such as electoral rolls or passports;

vii Section 7 of the Aadhaar Act is applicable only to such subsidies, benefits and services, for which the entire expenditure is directly incurred from the Consolidated Fund of India or from which the entire receipts directly form part of the Consolidated Fund of India;

viii Use of Aadhaar as the sole identity will not prevent pilferage and diversion of funds and subsidies, as faulty identification is only one of the factors that contributes to it; and

ix The Aadhaar project conditions the grant of essential benefits upon the surrender of individual rights.

Mr Gopal Subramanium, learned Senior Counsel, made the following submissions:

i The Aadhaar project violates dignity under Article 21 of the Constitution as recognised in the judgments- in **Puttaswamy**, **NALSA**[47] and **Subramanian Swamy**[48];

ii The Aadhaar project is unconstitutional as it seeks a waiver of fundamental rights;

iii The Aadhaar project violates the guarantees of substantive and procedural reasonableness under Articles 14,19 and 21;

iv Aadhaar perpetrates exclusion from social security schemes and is therefore discriminatory under Article 14;

v The Aadhaar Act lacks legitimacy in its object in so far as it validates a breach of fundamental rights retrospectively;

vi Rights and entitlements conferred under the Constitution cannot be based on algorithmic probabilities which UIDAI cannot control;

vii No consequence is prescribed for non-authentication under the Aadhaar Act;

viii The Aadhaar Act violates Part IX of the Constitution, which provides for decentralisation (to Panchayats), while the Aadhaar scheme strikes at the federal structure of the Constitution; and

[47] (2014) 5 SCC 438
[48] (2016) 7 SCC 221

ix Breaches under the Aadhaar Act cannot be cured.

Mr Arvind Datar, learned Senior Counsel has submitted:

i Rule 9 of the PMLA (Second Amendment) Rules, 2017 which requires mandatory linking of Aadhaar with bank accounts is unconstitutional and violates Articles 14, 19(1)(g), 21 and 300A of the Constitution, Sections 3, 7 and 51 of the Aadhaar Act, and is also ultra vires of the provisions of the PMLA Act, 2002 on the following grounds:

a. Under the impugned amended Rules, linkage of Aadhaar numbers to bank accounts is mandatory and persons not enrolling for Aadhaar cannot operate a bank account, which violates the spirit of Article 14 in entirety in so far it arbitrarily metes out unequal treatment based on unreasonable classification;

b The impugned Rules are violative of Article 19(1)(g) as the Rules refer to companies, firms, trusts, etc., whereas the Aadhaar Act is only to establish identity of “individuals”;

c Non-operation of a bank account, even for a temporary period, leads to deprivation of an individual's property and therefore constitutes a violation under Article 300A of the Constitution, which provides that deprivation can be done only by primary legislation; and

d The Rule has no nexus to the object of the PMLA Act, as the Act has no provision to make bank accounts non-operational;

ii Section 139AA of the Income Tax Act, 1961 is liable to be struck down as violative of Articles 14, 21 and 19(g) of the Constitution;

iii The decision in **Binoy Viswam** v **Union of India**[49] requires re-consideration in view of the nine judge Bench decision in **Puttaswamy**;

iv In view of serious deficiencies in the Aadhaar Act, there is a need for guidelines under Article 142 to protect *inter alia*, the right to privacy and to implement the mandate of the nine judge Bench in **Puttaswamy**;

v If the Aadhaar project is not struck down, it should be confined only for identification or authentication of persons who are entitled to subsidies, benefits and services for which expenditure is incurred from the Consolidated Fund of India;

vi Sections 2(g), 2(j) 7, 57 and 59 of the Aadhaar Act violate Articles 14, 21 and 300A of the Constitution; and

vii PMLA Rule 9 is arbitrary as it is contrary to the RBI Master Circular (issued in 2013), which provided a list of documents that were to be treated as 'identity proof', in relation to proof of name and proof of residence.

[49](2017) 7 SCC 59

Mr P Chidambaram, learned Senior Counsel argued that the Aadhaar Act could not have been passed as a Money Bill. Thus, he submitted:

i The only difference between financial bills and money bills is the term "only" in Article 110 of the Constitution which implies that the scope of money bills is narrower than the scope of financial bills and provisions relating to money bills must thus be construed strictly;

ii The Aadhaar Act, which was passed as a money bill, should be struck down since many of its provisions such as Section 57 have no relation to the nature of a Money Bill and bear no nexus to the Consolidated Fund of India;

iii Since Money Bills can only be introduced in the Lok Sabha, on account of the curtailment of the powers of the Rajya Sabha and the President, the relevant provisions must be accorded a strict interpretation;

iv While Article 110(3) provides that the decision of the Speaker of the Lok Sabha as to whether a Bill is a 'Money Bill' shall be final, the finality is only with regard to the Parliament and does not exclude judicial review; and

v Since the legislative procedure is illegal and the power of the Rajya Sabha has been circumvented to disallow legislative scrutiny of the

Aadhaar bill, provisions of the Act cannot be severed to save the Act and the Act is liable to be struck down as a whole by the Court.

Mr KV Vishwanathan, learned Senior Counsel made the following submissions:

i All acts done prior to the passage of the Act are void ab initio and are not saved or validated by Section 59. In any event, Section 59 is invalid;

ii Collection, storage and use of data under the Aadhaar project and Act are invalid for the following reasons:

a. The Aadhaar Act and the surrounding infrastructure has made the possession of Aadhaar de facto mandatory;
b. Compulsory collection of identity information violates various facets of the right to privacy - bodily privacy, informational privacy and decisional autonomy;
c. The Act is unconstitutional since it collects the identity information of children between 5-18 years without parental consent;
d. Centralised storage of identity information and the unduly long period of retention of transaction data and authentication records is disproportionate;

e. The Act and Regulations preclude Aadhaar number holders from accessing or correcting their identity information stored on the CIDR; and

f. The Act and Regulations lack safeguards to secure sensitive personal data.

iii Services like health related services, and those related to food, pensions and daily wages claimed under Section 7 of the Act have been denied because of biometric failure. Biometric infrastructure operates on a probabilistic system, which cannot be 'one hundred percent infallible'. Thus, the State needs to take steps to prevent the denial of benefits by adopting alternate methods for verification of identity. This is absent at present, resulting in a violation of Articles 14 & 21;

iv No provision is made for a hearing against omission and deactivation of the Aadhaar number, which violates the principles of natural justice; and

v Sections 2(g), 2(j), 2(k) and 23(2) of the Aadhaar Act suffer from excessive delegation and the allied regulations are vague, manifestly arbitrary and unreasonable.

Mr Anand Grover, learned Senior Counsel has submitted thus:

i The Aadhaar project extends far beyond the scope of the Aadhaar Act with no procedural safeguards. Hence it violates Article 21 in as much as it is without the support and sanction of law. The data collected is unauthorised, excessive and being illegally shared;

ii The use of biometric technology to establish identity is uncertain, unproven and unreliable leading to exclusion and a violation of Articles 14 and 21;

iii The lack of security in the Aadhaar project violates the right to privacy under Article 21;

iv Excessive powers have been delegated to the UIDAI through the Aadhaar Act; and

v Sections 33(2) and 57 of the Act are vague, overbroad and constitutionally invalid.

Ms Meenakshi Arora, learned Senior Counsel contended that:

i The general and indiscriminate retention of personal data, including meta-data, and the ensuing possibility of surveillance by the State has a chilling effect on fundamental rights like the freedom of speech and expression, privacy, and dignity;

ii Making Aadhaar the sole means of identification for various services impinges upon dignity as it amounts to requiring a license for the exercise of fundamental rights; and

iii The Aadhaar project does not contain any specific provisions for data protection, apart from a mere general obligation on UIDAI, which is a violation of the obligation of the State to ensure that the right to life, liberty, dignity and privacy of every individual is not breached under Part III of the Constitution.

Mr Sajjan Poovayya, learned Senior Counsel has urged the following submissions:

i The Aadhaar Act fails to satisfy the constitutional test of a just, fair and reasonable law;

ii Maintenance of Aadhaar records by the State under Section 32 is an unwarranted intrusion by the State;

iii Use of personal information under Section 33 is an unwarranted intrusion by the State;

iv Section 57 of the Act is contrary to the principle of purpose limitation; and

v Sections 2(g) and 2(j), the proviso to Section 3(1), Section 23(2)(g) and Section 23(2)(n) read with Section 54(2)(l), and Section 29(4) of the Act suffer from the vice of excessive delegation.

Mr CU Singh, learned Senior Counsel, argued that the rights of the child are violated through the Aadhaar project. A child has no right to give consent or to enter into a contract. A child in India, under law, has no power or right to bind herself to anything, to consent or enter into contracts. In this background, there is no compelling state interest to mandate Aadhaar for children. The fundamental right of a child to education cannot be made subject to production of Aadhaar. These requirements are not only contrary to domestic legislation protecting the rights of children but also against India's international obligations. Learned counsel also spoke of the violation of the rights of homeless people who are denied benefits due to the lack of a fixed abode.

Mr Sanjay Hegde, learned Senior Counsel has urged that since there is no 'essential practice' involved, exemptions must be allowed from the mandatory nature of the Aadhaar Act on the grounds of freedom of conscience under Article 25 of the Constitution.

Ms Jayna Kothari, learned Counsel arguing on behalf of an intervenor organization for transgender persons and sexual minorities urged that the

Aadhaar Act discriminates against sexual minorities. Aadhaar Regulations require demographic information. The enrolment form has a third gender, but there is no uniformity across the board, and the documents that have to be produced to get an Aadhaar card do not always have that option. Aadhaar is being made mandatory for almost everything but transgender persons cannot get an Aadhaar because they do not have the gender identity documents that Aadhaar requires. This non-recognition of gender identity leads to denial of benefits which is violative of both Articles 14 and 21.

It has also been argued before us in an intervention application that denial of Aadhaar to Non-Resident Indians leads to discrimination when NRIs seek to avail of basic services in India.

C.2 Respondents' submissions

Mr KK Venugopal, Learned Attorney General for India, has submitted thus:

i. For the period prior to coming into force of the Aadhaar Act, because of the interim orders passed by the SC, obtaining an Aadhaar number or enrollment number was voluntary, and hence there was no violation of any right;

ii. Section 59 of the Aadhaar Act protects all actions taken from the period between 2010 till the passage of the Aadhaar Act in 2016;

iii. The judgments in *MP Sharma* and *Kharak Singh* being those of 8 and 6 judges respectively, holding that the right to privacy is not a fundamental right, judgments of smaller benches delivered during the period upto **Puttaswamy** would be *per incuriam*. Hence, the State need not have proceeded on the basis that a law was required for the purpose of getting an Aadhaar number or an enrolment number. As a result, the administrative actions taken would be valid as well as the receipt of benefits and subsidies by the beneficiaries;

iv. Subsequent to the Aadhaar Act, the petitioners would have to establish that one or more of the tests laid down by the nine judge bench in **Puttaswamy** render the invasion of privacy resulting from the Aadhaar Act unconstitutional. The tests laid down in **Puttaswamy** have been satisfied and hence the Aadhaar Act is not unconstitutional for the following reasons:

a. The first condition in regard to the existence of a law has been satisfied;

b. Legitimate state interests such as preventing the dissipation of social welfare benefits, prevention of money laundering, black money and tax evasion, and protection of national security are satisfied through the Act;

c. The Aadhaar Act satisfies the test of proportionality by ensuring that a "rational nexus" exists between the objects of the Act and the means adopted to achieve its objects; and

d. For the purpose of testing legitimate State interest and proportionality, the Court must take note of the fact that each one of the subsidies and benefits under Section 7 is traceable to rights under Article 21 of the Constitution - such as the right to live with human dignity, the right to food, right to shelter, right to employment, right to medical care and education. If these rights are juxtaposed with the right to privacy, the former will prevail over the latter.

v. The Aadhaar Act was validly passed as a Money Bill on the following grounds:

a. The term 'targeted delivery of subsidies' contemplates an expenditure of funds from the Consolidated Fund of India, which brings the Aadhaar Act within the purview of a Money Bill under Art. 110 of the Constitution;

b. Sections 7, 24, 25 and the Preamble of the Act also support its classification as a Money Bill;

c. The Aadhaar Act has ancillary provisions, but they are related to the pith and substance of the legislation which is the targeted delivery of subsidies and benefits; and

d. Section 57 of the Act is saved by Article 110 (1) (g) of the Constitution as it is a standalone provision and even if a Bill is not covered under

clauses (a) to (f) of Article110(1), it can still be covered under Article110 (1) (g).

Mr Tushar Mehta, learned Additional Solicitor General, submitted:

i. Section 139AA of the Income Tax Act, was examined in **Binoy Viswam** in the context of Article 19 and fulfills the three tests laid down under **Puttaswamy** as well as the test of manifest arbitrariness laid down in **Shayara Bano** v **Union of India**[50];

ii. The demographic information that is required for Aadhaar enrollment is already submitted while obtaining a PAN card and therefore individuals do not have a legitimate interest in withholding information;

iii. Linking Aadhaar to PAN is in public interest on the following grounds:
   a. The State has a legitimate interest in curbing the menace of black money, money laundering and tax evasion, often facilitated by duplicate PAN cards, and the linking of Aadhaar to the PAN card will ensure that one person holds only one PAN Card, thereby curbing these economic offences;
   b. Aadhaar-PAN linking is in public interest and satisfies the test of proportionality and reasonableness;

[50] (2017) 9 SCC 1

c. The individual interest gives way to a larger public interest and a statutory provision furthering state interest will take precedence over fundamental rights;

d. The Court must not interfere with the Legislature's wisdom unless the statutory measure is shockingly disproportionate to the object sought to be achieved;

e. India is a signatory to various international treaties under which it has obligations to take action to curb the menace of black money and money laundering in pursuance of which measures including the amendments to *inter alia* the Income Tax Act and the PMLA Act and Rules thereunder, have been brought about by the legislature;

f. Statutory provisions under Aadhaar Act and Income Tax Act are distinct and standalone. Moreover, the validity of one provision cannot be examined in the light of the other;

g. Ascribing a (mandatory or voluntary) character to the provisions of a statute is Parliament's prerogative and cannot be questioned by courts; and

h. Rule 9 of the amended PMLA Rules that mandates furnishing of an Aadhaar number to open a bank account is not *ultra vires* the Aadhaar Act. Similarly, the Rule that an existing bank account will become non-operational if not linked with Aadhaar within six months is not a

penalty but a consequence to render the accounts of money launderers non-operational.

Mr Rakesh Dwivedi, learned Senior Counsel, has submitted:

i. The right to privacy exists when there is a reasonable expectation of privacy. However, this reasonable expectation of privacy differs from one dataset to another since the Aadhaar Act draws a distinction between demographic information, optional demographic information (eg. mobile number), core biometric information (fingerprints and iris scans) and biometric information such as photographs;

ii. Alternatively, the applicability of Article 21 has to be confined and limited to core biometric information;

iii. Fundamental rights are not absolute and can be restricted if permitted specifically. Article 21 expressly envisages deprivation by laws which seek to carry out legitimate objectives and are reasonable and proportionate;

iv. The Aadhaar Act does not cause exclusion because if authentication fails after multiple attempts, then the subsidies, benefits and services, can be availed of by proving the possession of an Aadhaar number, either by

producing the Aadhaar card or by producing the receipt of the application for enrolment and producing the enrolment ID number;

v. Section 7 of the Aadhaar Act protects the right to human dignity recognized by Article 21 of the Constitution by providing services, benefits and subsidies. The Aadhaar Act is a welfare scheme in pursuance of the State's obligation to respect the fundamental rights to life and personal liberty; to ensure justice (social, political and economic) and to eliminate inequality (Article 14) with a view to ameliorate the lot of the poor and the Dalits;

vi. Socio-economic rights must be read into Part III of the Constitution since civil and political rights cannot be enjoyed without strengthening socio - economic rights;

vii. A welfare State has a duty to ensure that each citizen has access at least to the basic necessities of life. The idea of a socialist state under a mandate to secure justice- social, economic and political - will be completely illusory if it fails to secure for its citizens the basic necessities in life. There cannot be any dignity for those who suffer starvation, subjugation, deprivation and marginalization and those who are compelled to do work which is intrinsically below human dignity;

viii. The Aadhaar number does not convert individuals to numbers. The Aadhaar number is necessary for authentication and it is solely used for that purpose. The petitioners have conflated the concepts of identity and identification. Authentication through a number is merely a technological requirement which does not alter the identity of an individual;

ix. Even if there is a conflict between the right to privacy and the right to food and shelter, the Aadhaar Act strikes a fair balance. The Aadhaar Act ensures human dignity and the right to life and liberty, hence there would be no reasonable expectation of privacy and autonomy;

x. The requirement to obtain an Aadhaar number under the Aadhaar Act does not reflect a lack of trust in citizens. Authentication by the State does not presume that all its citizens are dishonest. The provisions of the Aadhaar Act are merely regulatory in nature - similar to the process of frisking at airports or other offices - since there is no effective method to ensure targeted delivery;

xi. The “least intrusive test” is not applicable in the present case. The requirement that the least intrusive means of achieving the State object must be adopted, has been rejected by Indian courts in a catena of decisions as it involves a value judgment and second guessing the wisdom of the legislature. Such a test violates the separation of powers between the legislature and the judiciary;

xii. Even assuming that the ‘least intrusive method’ test applies, the exercise of determining the least intrusive method of identification is a technical exercise and cannot be undertaken in a court of law;

xiii. The Petitioners who have furnished smartcards as an alternative to the Aadhaar card, have not established that smartcards are less intrusive than the Aadhaar card authentication process;

xiv. The ‘strict scrutiny test’ does not apply to the Aadhaar Act. That test is conceptualised in the United States, to be only applied to ‘suspect classifications’;

xv. Section 7 of the Aadhaar Act does not involve any waiver of fundamental rights;

xvi. There can be no assumption of mala fide against the government or the legislature. A mere possibility of abuse is not a ground to invalidate the Aadhaar Act;

xvii. Through Section 57, Parliament intended to make the use of the Aadhaar number available for other purposes due to the liberalization and privatization of the economy in areas earlier occupied by the government and public sector. Many private corporate bodies are operating parallel to and in competition with the public sector such as in banking, insurance,

defence, and health. These are core sectors absolutely essential for national integrity, to the national economy and the life of people;

xviii. Sections 2(g), and (j) read with Section 54(2)(a) and Section 54(1) do not suffer from excessive delegation of power to UIDAI and there are sufficient guidelines coupled with restrictions. The regulation making power of the Authority under the Act is limited by the use of the expression 'such other biological attribute' which will be interpreted *ejusdem generis* with the categories of information mentioned before namely, fingerprints and iris scan. These categories have certain characteristics: firstly, they do not contain genetic information; secondly, they are non-intrusive; thirdly, apart from carrying out authentication they do not reveal any other information of the individual; fourthly, these are modes of identification used for identifying a person even without digital technology; fifthly, they are capable of being used for instantaneous digital authentication; and sixthly, they are biological attributes enabling digital authentication. The addition of biological attributes, under Section 54, must mandatorily be laid before the Parliament under Section 55. This is an additional check on the regulation making power of UIDAI;

xix. Under Section 2(k), which defines demographic information, certain sensitive categories of information such as 'race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history' of

the person are excluded. The term 'other relevant information' has to be construed *ejusdem generis* and would have to be necessarily demographic in nature as contrasted with biometric information;

xx. Aadhaar is necessary, as 3% of India's GDP amounting to trillions of rupees is allocated by Governments towards subsidies, scholarships, pensions, education, food and other welfare programmes. But approximately half of if does not reach the intended beneficiaries. Aadhaar is necessary for fixing this problem as no other identification document is widely and commonly possessed by the residents of the country and most of the other identity documents do not enjoy the quality of portability;

xxi. The enrolment and authentication processes under the Aadhaar Act are strongly regulated so that the data is secure;

xxii. The security of the CIDR is also ensured through adequate measures and safeguards;

xxiii. The Aadhaar Act ensures that UIDAI has control over the requesting entity during the authentication process;

xxiv. Enrolment Regulations ensure that the requirement of informed consent of individuals is fulfilled while securing the Aadhaar card in the following ways:

a. Firstly, the resident is given an opportunity of verifying his or her information for accuracy before uploading;
b. Secondly, the details and the supporting documents are provided by the resident, or an introducer (in specific cases);
c. Thirdly, the enrolling agency is obliged to inform the individual about the manner in which the information shall be used, the nature of recipients with whom the information is to be shared during authentication; and the existence of a right to access information, the procedure for making request for such access and details of the person/ department to whom a request can be made; and
d. Fourthly, the uploading of information is done in the presence of the individual.

xxv. When an individual makes a choice to enter into a relational sphere then his or her choice as to mode of identification would automatically get restricted on account of the autonomy of the individuals or institution with whom they wish to relate. This is more so where the individual seeks employment, service, subsidy or benefits;

xxvi. The Central government has the power to direct the linking of Aadhaar card, with SIM card, as it is proportional to the object sought to be achieved in the interest of national security;

xxvii. Regarding the process of authentication and metadata retained under the Act, it is submitted:

a. The only purpose of the Aadhaar project is authentication and there is no power under the Act to analyze data;
b. The Aadhaar Act does not involve big data or learning algorithms. It merely utilizes a matching algorithm for the purpose of authentication;
c. Metadata contemplated is process or technical metadata and does not reveal anything about the individual. Section 2(d) of the Act defines “authentication record” to mean the record of the time of authentication, identity of the RE and the response provided by the Authority”, and the relevant authentication regulation, Regulation 26, does not go beyond the scope of Section 2(d) of the Act;
d. Moreover, Regulation 26 and Section 32(3) of the Act prohibit the Authority from collecting or storing any information about the purpose of authentication; and
e. Only limited technical metadata is required to be stored in an effort to exercise control over REs by way of audits.

xxviii. Regarding the security of the Aadhaar data, it is submitted:

a. The provisions of the Information Technology Act, 2000 and the punitive measures provided there are made applicable to Aadhaar data under Section 30 of the Aadhaar Act; and

b. Anyone attempting to gain unauthorized access to the CIDR faces stringent punishment, including imprisonment upto 10 years.

xxix. On the control exercised by the Authority over the Requesting Entities (RE), the following was urged before the Court:

a. The standard of control exercised by the Authority on the Requesting Entities is ‘fair and reasonable’ as laid down under Article 21 of the Constitution;

b. This control includes requirements that the RE’s procure the fingerprint device from vendors controlled by the Authority, with the Authority also providing the hardware and software of the device. The device is subject to quality checks, and must be certified by the Authority before being used by the RE. The Authority also takes measures to ensure that data is sent to it in an encrypted form;

c. The license is given to the RE from the Authority only after an audit of the RE is conducted, and the audit report is approved; and

d. The data collected by these REs is segregated and there exists no way of aggregating this data. During authentication requests, the full identity information of the individual will never be transmitted back to the REs by the Authority as there exists a statutory bar from sharing Biometric information under Sections 29 (1) (a) and 29(4) of the Act.

xxx. UIDAI has entered into licensing agreements with foreign biometric solution providers (BSP) for software. Even though the source code of the software is retained by the BSP as it constitutes their intellectual property, the data in the server rooms is secure as the software operates automatically and the biometric data is stored offline. There is no opportunity available to the BSP to extract data as they have no access to it;

xxxi. Prior to the enactment of the Aadhaar Act, the Aadhaar project was governed by the provisions of the Information Technology Act, 2000. Section 72A of the Information Technology Act, 2000 provides for punishment for disclosure of information in breach of law or contract;

xxxii. The architecture of the Aadhaar Act does not enable any real possibility, proximate or remote, of mass surveillance in real time by the State;

xxxiii. The giving of identity information and undergoing authentication has no direct and inevitable effect on Article 19(1)(a). Alternatively, even if Article 19(1)(a) is attracted, Article 19(2) would protect Section 7 of the Aadhaar Act as it has a direct and proximate nexus to public order and security of the State;

xxxiv. In response to the argument that the requirements of Aadhaar number and authentication for benefits, services and subsidies would be ultra

vires Article 243-G and items 11, 12, 16, 17, 23, 25 and 28 of the XIth Schedule, it is submitted that the Panchayats get only such powers as are given to it by the legislature of the State. Article 243-G is merely enabling. There is no compulsion upon the State to endow the Panchayats with powers relating to the items specified in the XIth Schedule;

xxxv. On the validity and purpose of Section 57, it is urged:

a. Section 57 is not an enabling provision. It merely provides, as it states, that the provisions of the Act would not prevent the use of Aadhaar for other purposes;

b. However, Section 57 imposes a limitation on any such use for other purposes, that the use must be sanctioned by any law in force or any contract;

c. Another limitation is presented by the proviso to Section 57, which says that the use of the Aadhaar number shall be subject to the procedure and obligations under Section 8 and Chapter VI, which would necessarily also subject it to the operation of Chapter VII (dealing with Offences & Penalties) of the Act;

d. Under Section 57, the State, a body corporate or any other person cannot become Requesting Entities unless the limitations provided for under Section 57 are complied with;

e. Section 57 imposes limitations, and the use is backed by authentication, protection of information and punitive measures;

f. The expressions 'pursuant to any law or any contract', and 'to this effect'- necessarily entail that where the State makes a law or any body corporate enters into a contract, the law or contract should be prior in point of time to the making of any application for becoming a Requesting Entity or a Sub-Authentication User Agency under Regulation 12 of the Authentication Regulations; and

g. A large number of small service providers simply cannot become Requesting Entities under Section 57, as they will not meet the rigorous standard demanded by the eligibility conditions which are prescribed by the Regulations to become Authentication User Agencies (AUA)/ KYC User Agencies (KUA). Therefore, this provision does not create a situation whereby the common man is required to undergo authentication in all activities.

xxxvi. The Aadhaar Act is not exclusionary but inclusionary since it provides all citizens the bare necessities for a dignified existence;

xxxvii. Having the option to opt-out is not a constitutional requirement.

Mr Neeraj Kishan Kaul, learned Senior Counsel, made the following submissions:

i. Aadhaar is a speedy and reliable tool for identification and authentication and there is no reason to hold it invalid;

ii. Private entities and AUAs/KUAs that have built their businesses around it should be allowed to use Aadhaar authentication services;

iii. Section 57 is an enabling provision and private players should be given the choice to use the Aadhaar authentication services as a tool for verification if there is a consensus between private players' and their customers;

iv. Aadhaar authentication has benefited women in villages and migrants and increased the reach of microfinance institutions, thus reducing predatory financing; and

v. A statute cannot be struck down on the ground that there is scope for misuse.

Mr Jayant Bhushan, learned Senior Counsel appearing for the Reserve Bank of India urged the following submissions before the Court:

i. RBI, in exercise of its powers under the Banking Regulation Act, 1949 and Rule 9 of the PMLA Rules, 2005 issued an amended Master Circular on April 20, 2018 which mandates that Aadhaar has to be submitted to a Reporting Entity. This circular conforms with the PMLA rules;

ii. Rule 9(14) of the PMLA Rules provides that the Regulator- the RBI in this case, lay down guidelines incorporating the requirements of sub-rules 9(1)-(13), which would include enhanced or simplified measures to verify identity; and

iii. The requirement of submission of Aadhaar to the RE is in exercise of this power under Rule 9(14).

Mr Gopal Sankarnarayanan, learned counsel, has submitted:

i. The Aadhaar Act as a whole does not violate the fundamental right to privacy;

ii. The factors that save the Aadhaar Act from failing the proportionality test are (a) Voluntariness to subject one 's identity information to obtain the Aadhaar ; (b) Informed consent when such identity information is utilized; and (c) A draw on the Consolidated Fund of India;

iii. Right to identity is a fundamental right as a part of the right to dignity, which is being realized by the Aadhaar Act;

iv. The right to identity is also recognized under India's international obligations under instruments such as the UDHR and ICCPR;

v. In view of the large scale enrolments that have already taken place and the expenditure incurred by the Government out of public funds, it would

be in overarching public interest to give Section 59 full effect. If this were not done, the only avenue available to the Government would be to undertake the mammoth enrolment task all over again under a new regime, affording only a pyrrhic victory to the Petitioners, while there would be substantial revenue losses to the Government and deprivation of beneficial schemes to those eligible, in the meanwhile;

vi. Certain provisions of the Aadhaar Act have to be struck down or read down so that the Act as a whole can continue to serve its essential purpose - namely Sections 47, Section 8(4) and Section 29(2) of the Act; and

vii. Section 139AA of the Income Tax Act, 1961 violates Article 14 and 21 of the Constitution.

Mr Zoheb Hossain, learned Counsel, made the following submissions:

i. The right to privacy cannot be asserted vicariously on behalf of others in a representative capacity in a Public Interest Litigation, because unlike other constitutional rights, right to privacy is a personal right. No Section 7 beneficiary has claimed a violation of their right to privacy despite the pendency of the petitions for 6 years before this Court and therefore, the Petitioners' challenge, in a representative capacity, to section 7 on the

ground of a violation of the right to privacy of third parties is not maintainable;

ii. There is no increased threat to privacy due to Aadhaar at the level of requesting entities (RE) for the following reasons:

a. REs are already in possession of personal information of individuals and inclusion of Aadhaar does not in any manner increase the threat to privacy;

b. Any information disclosed by REs will not be on account of Aadhaar and will have to be dealt with under domain specific legislations, or a data protection regime or agreements between the REs and their customers; and

c. REs have data of their own customers and not of other REs' customers, so there is no possibility of surveillance.

iii. Safeguards against disclosure of information in the Aadhaar Act are superior to the safeguards laid down in the **PUCL** case[51]. Sections 8, 28 and 29 along with Chapter VII which deals with Offences and Penalties, provide for protection of information and Section 33 lays down a strict procedure for disclosure. Even though the Aadhaar Act is not required to meet the same standard as laid down in **PUCL**, the safeguards in the Act are not only adequate with regard to identity information and authentication records, but far exceed the safeguards laid down **PUCL**;

[51] (2011) 14 SCC 331

iv. The petitioners cannot contend that Section 33(2) of the Aadhaar Act goes against the principles of natural justice and is disproportionate (as it does not define the term “national security”) for the following reasons:

a. What is in the interest of “national security” is not a question of law but that of policy lying in the executive domain; and

b. Principles of natural justice cannot be observed strictly in a situation implicating national security. In such cases, it is the duty of the court to read into and provide for statutory exclusion.

v. The laws, which are under challenge, are a part of a concerted scheme to promote redistributive justice and ensure substantive equality, in furtherance of Articles 14, 38, 39B and 39C. These laws ensure a more transparent and a cleaner system, root out revenue leakages and evasion of taxes, thereby giving genuine beneficiaries their rightful share in subsidies;

vi. The object of the Aadhaar Act, contrary to what the petitioners have argued, is totally unrelated to suppression of freedom of speech and any incidental effect, if at all, would not implicate the right under Article 19(1)(a);

vii. The petitioners cannot contend that Section 47 of the Aadhaar Act is arbitrary or unreasonable for the following reasons:

a. The offences and penalties under the Act are intended to maintain the purity of data of the Aadhaar number holder and the integrity of the CIDR, which are integral in achieving the object of the Act;

b. Enrolment, storage of data in CIDR, and authentications are so vast and inherently technical that any breach of the provisions, can be effectively dealt with by the UIDAI;

c. The individual has not been left remediless, as he/she can make a complaint to the UIDAI directly or through the grievance redressal centre [Regulation 32 of the Aadhaar (Enrolment and Update) Regulations, 2016]. After a complaint has been made, the UIDAI would be obliged to examine the complaint and accordingly lodge a complaint in a Court in terms of Section 47 of the Aadhaar Act;

d. Section 56 of the Aadhaar Act makes it clear that application of other laws, like the IT Act, is not barred.

viii. Aadhaar must be made mandatory under Section 7 of the Aadhaar Act for the following reasons:

a. Because of the involvement of biometrics, it is almost impossible for one person to obtain two Aadhaar numbers. This will help in checking the entry of fake and duplicate beneficiaries into any welfare scheme;

b. Other methods which were employed over the last 70 years to check duplication, siphoning of money in welfare schemes, large-scale tax evasion, generation of black money, and appearance and re-

appearance of duplicates, have turned out to be futile. If Aadhaar is made voluntary, the same problems are likely to creep back into the system; and

c. The State is bound to deploy the best technology available to it to ensure proper allocation of resources as there is a constitutional mandate upon the State under Article 14 to efficiently utilize its resources.

ix. There is no conflict between the Aadhaar Act and the Income Tax Act as they are both stand alone laws and their scope of operation is different;

x. Through the Aadhaar Act, the State is furthering the following obligations under Part III and Part IV of the Constitution and international obligations:

a. The State has a positive obligation for securing socio-economic rights like the basic right to food, shelter and livelihood of people arising out of Article 21, even though it is worded negatively;

b. The Supreme Court has observed that civil & political rights and socio-economic rights in India are placed on the same pedestal **[PUCL]**. Aadhaar is a means of achieving the latter set of rights. The proportionality analysis would therefore require a balancing of rights in this context;

c. Articles 38, 39(b), (c), (e), (f), 41, 43, 47 and 51(c) impose a constitutional mandate on the State to ensure effective and efficient utilization of public resources;

d. The State is the trustee of public resources towards people, and inaction of the State to plug the continuous leakage of public resources and revenues would violate both, the principle of non-arbitrariness and reasonableness envisaged by Article 14 as well as the constitutional doctrine of public trust; and

e. The creation of Aadhaar infrastructure and enactment of the Aadhaar Act is a step towards the government pursuing India's international obligations under the ICESCR.

xi. While testing proportionality, reasonableness of a restriction has to be determined in an objective manner from the standpoint of the interests of the general public and not from the perspective of an individual right bearer claiming invasion[52]; and

xii. With regard to the alleged conflict between Section 29(2) of the Aadhaar Act and Section 4(b)(xii) of the RTI Act, the former cannot be struck down as unconstitutional for the following reasons:

[52] Modern Dental College and Research Centre v State of Madhya Pradesh, (2016) 7 SCC 353.

a. A provision can be struck down only if it is in violation of the Constitution or if the legislature lacks competence, not on the ground that it is in conflict with another law;

b. In any case, the obligations of public authorities under both these provisions are different, as the public authority under the RTI Act can publish the details of beneficiaries from the existing database and the information received by the UIDAI is not required to be shared or displayed publicly. However, if any information is displayed publicly, it can be challenged by an aggrieved person on the ground of privacy which would be completely unrelated to the present challenge;

c. The two laws operate in their distinct fields and there is no conflict between them; and

d. A conflict between two statutes is required to be reconciled through harmonious construction. However, since there is no conflict between these two laws, there is no need for harmonious construction.

D Architecture of Aadhaar: analysis of the legal framework

39 The architecture of the Aadhaar Act envisages the creation of a unique identity for residents on the basis of demographic and biometric information. The Act envisages a process of identification by which the unique identity

assigned to each individual is verified with the demographic and biometric information pertaining to that individual which is stored in a centralised repository of data known as the Central Identities Data Repository (CIDR). The former part of the legislative design is implemented by its regulatory provisions governing enrolment[53] of individuals who would be allotted a unique identity number. The latter part of the legislative design consists of the process of 'authentication'.

40 In order to facilitate an understanding of the key aspects of the law, Section 2 provides a dictionary of meanings. 'Aadhaar number' is defined in Section 2(a) as the identification number issued to the individual under sub-section (3) of Section 3. The individual to whom an Aadhaar number is issued is described in Section 2(b) as the 'Aadhaar number holder'. The expression 'authentication' is defined in Section 2(c) thus:

> **"**(c) **"Authentication"** means the process by which the Aadhaar number alongwith demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness or lack thereof, on basis of information available with it."

Section 2(d) speaks of the 'authentication record' as the record of the time of authentication, the identity of the requesting entity and the response provided by UIDAI. The crucial definitions are those of 'biometric information', 'core

[53] Section 2(m) states: "enrolment" means the process, as may be specified by regulations, to collect demographic and biometric information from individuals by the enrolling agencies for the purpose of issuing Aadhaar numbers to such individuals under this Act.

biometric information', 'demographic information' and 'identity information'. These are as follows:

> "(g) "biometric information" means photograph, finger print, Iris scan, or other such biological attributes of an individual as may be specified by regulations;
>
> ...
>
> (j) "core biometric information" means finger print, Iris scan, or such other biological attribute of an individual as may be specified by regulations;
>
> (k) "demographic information" includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history.
>
> ...
>
> (n) "identity information" in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information."

The largest subset of the above definitions consists of 'identity information' which is defined in an inclusive sense to comprehend the Aadhaar number, biometric information and demographic information. Demographic information is defined as information related to the name, date of birth and address and other information pertaining to an individual as is specified by the regulations. Significantly, Section 2(k) excludes, by a mandate, race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history from the purview of demographic information. Biometric information consists, under Section 2(g), of the photograph, fingerprint, Iris scan, or other such biological attributes of an individual as may be specified by regulations. Core biometric information in Section 2(j) excludes photographs (which form part of biometric

information). Apart from photographs, other biometric information is comprehended within core biometric information and may be expanded to include other biological attributes specified in the regulations to be made under the Act.

41 The identity information of an individual is stored in a central depository. Section 2(h) defines "Central Identities Data Repository" as a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other related information. The CIDR is the backbone of the Aadhaar Act. All the information collected or created under the Act is stored in it. For the establishment and maintenance of the CIDR, it has been provided[54] under the Act that UIDAI may engage one or more entities, which can also perform any other functions as may be specified by regulations. The Act does not prohibit the engagement of private entities for the establishment and maintenance of the CIDR.

42 Section 3, pertains to the entitlement to obtain an 'Aadhaar Number', which forms a part of Chapter II titled 'enrolment'. Section 3 comprises of three parts: (i) an entitlement of every resident to obtain an Aadhaar number; (ii) a requirement of submitting demographic and biometric information to be enrolled; and (iii) a process of undergoing enrolment. Section 3 provides thus:

[54] Section 10, Aadhaar Act

> "Section (3): Aadhaar Number.-
>
> (1) Every resident shall be entitled to obtain an Aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment:
> Provided that the Central Government may, from time to time, notify such other category of individuals who may be entitled to obtain an Aadhaar number.
>
> (2) The enrolling agency shall, at the time of enrolment, inform the individual undergoing enrolment of the following details in such manner as maybe specified by regulations, namely:-
>
> (a) The manner in which the information shall be used;
> (b) The nature of recipients with whom the information is intended to be shared during authentication; and
> (c) The existence of a right to access information, the procedure for making requests for such access and details of the person or department in-charge to whom such requests can be made.
>
> (3) On receipt of the demographic information and biometric information under sub-section (1), the Authority shall, after verifying the information, in such manner as may be specified by regulations, issue an Aadhaar number to such individual."

Significantly, sub-section (1) of Section 3 recognises an entitlement, of every resident[55] to obtain an Aadhaar number. An entitlement postulates a right. A right contemplates a liberty, for it is in the exercise of the liberty that the individual asserts a right. What is a matter of an entitlement is evidently a matter of option and not a compulsion. That constitutes the fundamental postulate of Section 3. However, the entitlement to obtain the Aadhaar

[55] Section 2(v) states: "resident" means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment

number is conditioned by the requirement of submitting demographic and biometric information and participating in the process of enrolment.

43 The collection of demographic and biometric information is carried out by an enrolling agency. “Enrolling agency” has been defined under Section 2(l) of the Act as an agency, appointed by UIDAI or a Registrar[56], for collecting demographic and biometric information of individuals under the Act. The enrolling agency need not be an entity of the state. The definition opens the space for engagement of private entities in the collection of individual information for the process of enrolment. The enrolling agencies have to set up enrolment centers and they have to function in accordance with the procedure specified by UIDAI.[57] Sub-section (2) of Section 3 requires the enrolling agency to disclose to the individual, who is undergoing enrolment, three important facets. The first is the manner in which the information which is disclosed by the individual would be used. The second relates to the nature of the recipients with whom the information is likely to be shared during the course of authentication. The third is founded upon the individual’s right of access to the information disclosed. All these three facets are crucial to the legislative design because they try to place individual autonomy at the forefront of the process. An individual who discloses biometric and demographic information has a statutory entitlement to fully understand how the information which is disclosed is going to be used and with whom the

[56] Section 2(s) states: “Registrar” means any entity authorised or recognised by the Authority for the purpose of enrolling individuals under this Act
[57] Regulation 7, Aadhaar (Enrolment and Update) Regulations, 2016

information is likely to be shared during authentication.[58] Access of the information supplied to the individual, it has been argued, is an integral feature of the design created by the statute. These three facets are conditions precedent to the disclosure of information by the individual. Before the individual does so, he or she must have a full disclosure which would enable them to form an informed decision on the exercise of the choice which underlies an entitlement to an Aadhaar number. The entitlement which is recognised by sub-section (1) is enforced by the mandatory requirements of sub-section (2). Before an Aadhaar number is issued, sub-section (3) requires the authority to verify the information disclosed, in the manner prescribed by regulations. The Act leaves it to regulations to specify how verification will be carried out.

44 Sections 4, 5 and 6 indicate the characteristics which are attributed to Aadhaar numbers, legislative recognition of the steps necessary to ensure financial inclusion and the requirement of periodical updation of information. Under Section 4, three important features attach to the possession of an Aadhaar number. The first is that the number is unique to one individual and to that individual alone. Once assigned, the Aadhaar number cannot be reassigned to any other individual. The second feature is that an Aadhaar number is random and bears no relation to the attributes or identity of its holder. The third feature of Section 4 is that once assigned, an Aadhaar number can be accepted as proof of identify of its holder “for any purpose”.

[58] Section 3(2), Aadhaar Act.

Under Section 5, UIDAI is under a mandate to adopt special measures to issue Aadhaar numbers to women, children, senior citizens, the differently abled, unskilled and unorganised workers, nomadic tribes, persons who do not have permanent places of abode and to other categories which may be defined by the regulations. Section 6 contains an enabling provision by which the authority may require holders to update their demographic and biometric information periodically, as specified under regulations. An Aadhaar number also does not, by itself, constitute a conferment of a right of citizenship, or domicile (Section 9).

45 Chapter III provides for Authentication. By virtue of Section 7, an enabling provision has been made by which the Union or state governments may **require** proof of an Aadhaar number for receiving subsidies, benefits and services for which the expenditure is incurred from (or the receipts form part of) the Consolidated Fund of India. Section 7 is in the following terms:

> "7. Proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc.- The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment:
>
> Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service."

Section 3 (as explained earlier) postulates an entitlement to an Aadhaar number. An entitlement envisages a right which may (or may not) be exercised by the resident. An entitlement is, after all, an option. Section 7, however, contemplates a **requirement**. It covers subsidies, benefits or services that are charged to the Consolidated Fund of India; the connect being either in regard to the source of expenditure or the receipts. The statutory definitions of the expressions 'benefit', 'service' and 'subsidy' are contained in clauses (f),(w) and (x) of Section 2 which provide as follows:

> "(f) "benefit" means any advantage, gift, reward, relief, or payment, in cash or kind, provided to an individual or a group of individuals and includes such other benefits as may be notified by the Central Government;"
>
> (w) "service" means any provision, facility, utility or any other assistance provided in any form to an individual or a group of individuals and includes such other services as may be notified by the Central Government;
>
> (x) "subsidy" means any form of aid, support, grant, subvention, or appropriation, in cash or kind, to an individual or a group of individuals and includes such other subsidies as may be notified by the Central Government."

46 Section 7 encapsulates a purpose, a condition and a requirement. The purpose incorporated in the provision is to establish the identity of an individual. The condition which it embodies is for the receipt of a subsidy, benefit or service for which the expenditure is incurred or the receipts form part of the Consolidated Fund of India. Where the purpose and condition are fulfilled, the central or state governments may require that the individual should (i) undergo authentication; or (ii) furnish proof of possession of an Aadhaar number; or (iii) provide proof of an application for enrolment where

the Aadhaar number has not been assigned. Three alternatives are stipulated in Section 7. Where the purpose and condition (noted above) are fulfilled, the individual has to undergo authentication. Alternately, the individual has to furnish proof that he or she possesses an Aadhaar number. However, if an Aadhaar number has not been assigned to the individual, he or she would have to make an application for enrolment. In a situation where no Aadhaar number has been assigned as yet, the proviso stipulates that alternate and viable means of identification would be provided to the individual for the delivery of subsidies, benefits or services. Section 7 indicates that while the central or state governments can mandate that an individual must undergo authentication as a condition for the receipt of a subsidy, benefit or service, a failure of authentication cannot be held out as a ground to deny benefits, subsidies or services. That is for the reason that in the absence of authentication, possession of an Aadhaar number would suffice. Moreover, even if an individual does not possess an Aadhaar number, the mandate of Section 7 would be subserved by producing an application for enrolment.

Section 3 which speaks of an entitlement to obtain an Aadhaar number stands in contrast to Section 7 under which an Aadhaar number may be required as a condition for the receipt of a subsidy, benefit or service. As an entitlement, Section 3 makes the possession of an Aadhaar number optional. Section 7 is an enabling power by which the central or state governments may make the requirement of an Aadhaar number compulsive or mandatory where a person

desires a subsidy, benefit or service for which expenditure is incurred from or the receipt of which forms part of the Consolidated Fund of India. Section 7 acts as an overriding provision over Section 3.

47 The manner in which an authentication is carried out is elaborated upon by Section 8. Section 8 is in the following terms:

> "**Authentication of Aadhaar number.-**
>
> (1) The Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder submitted by any requesting entity, in relation to his biometric information or demographic information, subject to such conditions and on payment of such fees and in such manner as may be specified by regulations.
>
> (2) A requesting entity shall –
>
> (a) unless otherwise provided in this Act, obtain the consent of an individual before collecting his identity information for the purposes of authentication in such manner as may be specified by regulations; and
>
> (b) ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication.
>
> (3) A requesting entity shall inform, in such manner as may be specified by regulations, the individual submitting his identify information for authentication, the following details with respect to authentication, namely:-
>
> (a) the nature of information that may be shared upon authentication;
>
> (b) the uses to which the information received during authentication may be put by the requesting entity; and
>
> (c) alternatives to submission of identity information to the requesting entity.
>
> (4) The Authority shall respond to an authentication query with a positive, negative or any other appropriate response sharing such identity information excluding any core biometric information."

As we have noticed earlier, authentication involves a process in which the Aadhaar number, together with the demographic or biometric information, is

submitted to the CIDR for verification and is verified to be correct or otherwise by the repository on the basis of the information available with it. Under sub-section (1) of Section 8 authentication has to be performed on a request submitted by a requesting entity. The expression 'requesting entity' is defined in Section 2(u) as follows:

> "(u) "requesting entity" means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication."

This definition also does not prohibit the engagement of private agencies for the process of authentication. Under sub-section (2) of Section 8, every requesting entity is bound to obtain the consent of the individual before collecting his or her identity information for the purpose of authentication. Moreover, the requesting entity must ensure that the identity information is submitted only for the purpose of authentication to the CIDR. Before the requesting entity submits the identity information for authentication, it is under a mandate of law to disclose (i) the nature of the information that may be shared upon authentication; (ii) the use to which information received during authentication may be put; and (iii) alternatives to the submission of identity information.[59] During the course of authentication, UIDAI is required to respond to an authentication query with a positive, negative or appropriate response sharing such identity information excluding core biometric information.[60] Core biometric information cannot be shared. The modes of

[59] Section 8(3), Aadhaar Act
[60] Section 8(4), Aadhaar Act

authentication are as mentioned in Regulation 4 of the Aadhaar (Authentication) Regulations 2016. It can be based on (i) demographic information; (ii) a one-time password with limited time validity; (iii) biometrics or (iv) multi-factor authentication (a combination of two or more of the above). The Requesting Agency chooses the mode according to its requirement.

48 UIDAI is the umbrella entity under the Aadhaar Act. The statutory backing to the authority of UIDAI to undertake the responsibility for the processes of enrolment and authentication and maintenance of CIDR has been provided under Chapter IV of the Act. Section 11 provides that the Central Government shall, by notification, establish UIDAI, a body corporate[61], to be responsible for the processes of enrolment and authentication and perform such other functions as are assigned to it under the Act. The composition of UIDAI has been provided under Section 12: a Chairperson (appointed on part-time or full-time basis); two part-time Members, and the chief executive officer who shall be the Member- Secretary, to be appointed by the Central Government. Section 23 enunciates the powers and functions of the UIDAI. Sub-section (1) of Section 23 requires UIDAI to develop the policy, procedure and systems for issuing Aadhaar numbers to individuals and to perform authentication. Section 23(2) provides an inclusive list of the powers and functions of UIDAI:

> "(2) Without prejudice to sub-section (1), the powers and functions of the Authority, *inter alia*, include—

[61] Section 11(2), Aadhaar Act

(a) specifying, by regulations, demographic information and biometric information required for enrolment and the processes for collection and verification thereof;

(b) collecting demographic information and biometric information from any individual seeking an Aadhaar number in such manner as may be specified by regulations;

(c) appointing of one or more entities to operate the Central Identities Data Repository;

(d) generating and assigning Aadhaar numbers to individuals;

(e) performing authentication of Aadhaar numbers;

(f) maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;

(g) omitting and deactivating of an Aadhaar number and information relating thereto in such manner as may be specified by regulations;

(h) specifying the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used;

(i) specifying, by regulations, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof;

(j) establishing, operating and maintaining of the Central Identities Data Repository;

(k) sharing, in such manner as may be specified by regulations, the information of Aadhaar number holders, subject to the provisions of this Act;

(l) calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of this Act of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act;

(m) specifying, by regulations, various processes relating to data management, security protocols and other technology safeguards under this Act;

(n) specifying, by regulations, the conditions and procedures for issuance of new Aadhaar number to existing Aadhaar number holder;

(o) levying and collecting the fees or authorising the Registrars, enrolling agencies or other service providers to

> collect such fees for the services provided by them under this Act in such manner as may be specified by regulations;
>
> (p) appointing such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act;
>
> (q) promoting research and development for advancement in biometrics and related areas, including usage of Aadhaar numbers through appropriate mechanisms;
>
> (r) evolving of, and specifying, by regulations, policies and practices for Registrars, enrolling agencies and other service providers;
>
> (s) setting up facilitation centres and grievance redressal mechanism for redressal of grievances of individuals, Registrars, enrolling agencies and other service providers;
>
> (t) such other powers and functions as may be prescribed."

Under Section 54, UIDAI is empowered to make regulations and rules consistent with the Act, for carrying out the provisions of the Act. Sub-section (2) of Section 54 provides that UIDAI may make regulations covering any of the following matters:

> "(a) the biometric information under clause (g) and the demographic information under clause (k), and the process of collecting demographic information and biometric information from the individuals by enrolling agencies under clause (m) of section 2;
>
> (b) the manner of verifying the demographic information and biometric information for issue of Aadhaar number under sub-section (3) of section 3;
>
> (c) the conditions for accepting an Aadhaar number as proof of identity of the Aadhaar number holder under sub-section (3) of section 4;
>
> (d) the other categories of individuals under section 5 for whom the Authority shall take special measures for allotment of Aadhaar number;
>
> (e) the manner of updating biometric information and demographic information under section 6;
>
> (f) the procedure for authentication of the Aadhaar number under section 8;

(g) the other functions to be performed by the Central Identities Data Repository under section 10;

(h) the time and places of meetings of the Authority and the procedure for transaction of business to be followed by it, including the quorum, under sub-section (1) of section 19;

(i) the salary and allowances payable to, and other terms and conditions of service of, the chief executive officer, officers and other employees of the Authority under sub-section (2) of section 21;

(j) the demographic information and biometric information under clause (a) and the manner of their collection under clause (b) of sub-section (2) of section 23;

(k) the manner of maintaining and updating the information of individuals in the Central Identities Data Repository under clause (f) of sub-section (2) of section 23;

(l) the manner of omitting and deactivating an Aadhaar number and information relating thereto under clause (g) of sub-section (2) of section 23;

(m) the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used under clause (h) of sub-section (2) of section 23;

(n) the terms and conditions for appointment of Registrars, enrolling agencies and other service providers and the revocation of appointments thereof under clause (i) of sub-section (2) of section 23;

(o) the manner of sharing information of Aadhaar number holder under clause (k) of sub-section (2) of section 23;

(p) various processes relating to data management, security protocol and other technology safeguards under clause (m) of sub-section (2) of section 23;

(q) the procedure for issuance of new Aadhaar number to existing Aadhaar number holder under clause (n) of sub-section (2) of section 23;

(r) manner of authorising Registrars, enrolling agencies or other service providers to collect such fees for services provided by them under clause (o) of sub-section (2) of section 23;

(s) policies and practices to be followed by the Registrar, enrolling agencies and other service providers under clause (r) of sub-section (2) of section 23;

> (t) the manner of accessing the identity information by the Aadhaar number holder under the proviso to sub-section (5) of section 28;
>
> (u) the manner of sharing the identity information, other than core biometric information, collected or created under this Act under sub-section (2) of section 29;
>
> (v) the manner of alteration of demographic information under sub-section (1) and biometric information under sub-section (2) of section 31;
>
> (w) the manner of and the time for maintaining the request for authentication and the response thereon under sub-section (1), and the manner of obtaining, by the Aadhaar number holder, the authentication records under sub-section (2) of section 32;
>
> (x) any other matter which is required to be, or may be, specified, or in respect of which provision is to be or may be made by regulations."

Section 11(1), read with Sections 23(2) and 54(2), indicates that UIDAI is the sole authority vested with the power and responsibility of carrying out numerous functions. These functions include:

(i) collection of demographic information and biometric information from individuals;

(ii) generating and assigning Aadhaar numbers to individuals;

(iii) performing authentication of Aadhaar numbers;

(iv) maintaining and updating the information of individuals in the CIDR;

(v) omitting and deactivating of an Aadhaar number;

(vi) specifying the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes;

(vii) specifying the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments;

(viii) specifying various processes relating to data management, security protocols and other technological safeguards under the Act;

(ix) setting up facilitation centres and mechanisms for the redressal of the grievances of individuals, Registrars, enrolling agencies and other service providers; and

(x) other functions prescribed by the Central government.

The Act does not set any limits within which the sole authority of UIDAI may operate. UIDAI has been conferred with discretionary powers as provided in the above provisions. The architecture of Aadhaar keeps UIDAI at the centre of all processes.

49 For the purpose of performing the functions of collecting, storing, securing, processing of information, delivery of Aadhaar numbers to individuals or performing authentication, clause (a) of Section 23(3) contemplates that UIDAI may enter into Memoranda of Understanding or agreements with the central or state governments, Union territories or other agencies. In discharging its functions, UIDAI may appoint, by notification, a number of Registrars, engage and authorise such agencies to collect, store, secure and process information or perform authentication or such other functions in relation to it, as may be necessary for the purposes of the Act

(Section 23 (3) (b)). For the efficient discharge of its functions, UIDAI may also engage consultants, advisors and other persons as may be required (Section 23(4)). These, like many other provisions, open the scope for the involvement of private entities in the Aadhaar project. This is also evident from Section 57 of the Act, which allows the use of the Aadhaar number, by the state, corporate entities or persons to establish the identity of an individual:

> "57. Act not to prevent use of Aadhaar number for other purposes under law.-
>
> Nothing contained in this Act shall prevent the use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or any body corporate or person, pursuant to any law, for the time being in force, or any contract to this effect:
>
> Provided that the use of Aadhaar number under this section shall be subject to the procedure and obligations under section 8 and Chapter VI."

50 The responsibility to ensure the security of identity information and authentication records of individuals has been placed on UIDAI.[62] UIDAI is also required to ensure confidentiality of identity information and authentication records of individuals,[63] except in circumstances, where disclosure of information is permitted by the Act.[64] Section 28(3) requires UIDAI to take all necessary measures to ensure that the information in its possession or control, including information stored in the CIDR, is secured and protected against access, use or disclosure not permitted under the Act or regulations, and against accidental or intentional destruction, loss or damage. For the purpose

[62] Section 28(1), Aadhaar Act
[63] Section 28(2), Aadhaar Act
[64] Section 33, Aadhaar Act

of maintaining the security and confidentiality of the information of individuals, UIDAI is also required, under Section 28(4), to:

> "(a) adopt and implement appropriate technical and organisational security measures;
>
> (b) ensure that the agencies, consultants, advisors or other persons appointed or engaged for performing any function of the Authority under this Act, have in place appropriate technical and organisational security measures for the information; and
>
> (c) ensure that the agreements or arrangements entered into with such agencies, consultants, advisors or other persons, impose obligations equivalent to those imposed on the Authority under this Act, and require such agencies, consultants, advisors and other persons to act only on instructions from the Authority."

Except where it has otherwise been provided in the Aadhaar Act, a burden is placed (under Section 28(5)) upon UIDAI, its officers, other employees (whether during service or thereafter), and any agency that maintains the CIDR not to reveal any information stored or the authentication record to anyone. An Aadhaar number holder, however, may request UIDAI to provide access to identity information excluding core biometric information in the manner as may be specified by regulations (proviso to Section 28(5)).

Section 29 puts restrictions on sharing of information, collected or created under the Act. Sub-section (1) of Section 29 provides that:

> "(1) No core biometric information, collected or created under this Act, shall be—
> (a) shared with anyone for any reason whatsoever; or
> (b) used for any purpose other than generation of Aadhaar numbers and authentication under this Act."

Sub-section (2) contemplates that the identity information, other than core biometric information, collected or created under the Act may be shared only in accordance with the provisions of the Act and in the manner as may be specified by regulations.

A burden is placed, under Section 29(3), upon a requesting entity to ensure that any identity information available with it, is neither used for any purpose, other than that specified to the individual at the time of submitting identity information for authentication; nor disclosed further, except with the prior consent of the individual to whom such information relates.

Sub-section (4) prohibits publishing, display or posting publicly of any Aadhaar number or core biometric information collected or created under the Act in respect of an Aadhaar number holder, except for such purposes as may be specified by the regulations. Section 30 contemplates that the biometric information collected and stored in an electronic form is to be deemed "sensitive personal data or information". The provision specifically relates to biometric information. The provision dilutes the protection that should be given to demographic information. Further, a statutory duty has been placed upon UIDAI to maintain authentication records in the manner and for a time period prescribed by regulations.[65] The issue of maintenance of authentication records by UIDAI has been contentious and is dealt in a subsequent section titled "Proportionality". A statutory right is provided to every Aadhaar number

[65] Section 32(1), Aadhaar Act

holder to obtain his authentication record in the manner specified by regulations.[66] Section 32(3) prohibits UIDAI (either by itself or through any entity under its control) to collect, keep or maintain any information about the purpose of authentication.

51 The Aadhaar Act allows disclosure of individual information in limited circumstances. The manner and purpose for which information of individuals, including identity information or authentication records, can be disclosed has been provided under Section 33 of the Act. Section 33 states:

> "(1) Nothing contained in sub-section (2) or sub-section (5) of section 28 or sub-section (2) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made pursuant to an order of a court not inferior to that of a District Judge:
>
> Provided that no order by the court under this sub-section shall be made without giving an opportunity of hearing to the Authority.
>
> (2) Nothing contained in sub-section (2) or sub-section (5) of section 28 and clause (b) of sub-section (1), sub-section (2) or sub-section (3) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government:
>
> Provided that every direction issued under this sub-section, shall be reviewed by an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology, before it takes effect:
>
> Provided further that any direction issued under this sub-section shall be valid for a period of three months from the

[66] Section 32(2), Aadhaar Act

> date of its issue, which may be extended for a further period of three months after the review by the Oversight Committee."

The Aadhaar Act provides two categories: a "court order" and "in the interest of national security", where the personal information of an individual can be disclosed.

Under Section 31, in case any demographic information or biometric information of an Aadhaar number holder is found to be incorrect, is lost or changes subsequently, the Aadhaar number holder is required to request UIDAI to make an alteration in his or her record in the CIDR in the manner specified by regulations. On receipt of a request for alteration of demographic or biometric information, UIDAI is vested with the power, subject to its satisfaction, to make alterations as required in the record relating to the Aadhaar number holder and to intimate the alteration to the holder. Sub-section (4) of Section 31 prohibits alteration of any identity information in the CIDR except in the manner provided in the Act or regulations made in this behalf.

52 Chapter VII provides offences and penalties. Under Section 34, a penalty has been provided for impersonation at the time of enrolment. Section 35 creates a penalty for impersonation of the Aadhaar number holder by changing demographic or biometric information. Section 37 provides a penalty

for disclosing identity information (which was collected in the course of enrolment or authentication).

Under Section 38, a penalty for unauthorised access to the CIDR has been provided. Section 38 provides thus:

> "Whoever, not being authorised by the Authority, intentionally,—
>
> (a) accesses or secures access to the Central Identities Data Repository;
>
> (b) downloads, copies or extracts any data from the Central Identities Data Repository or stored in any removable storage medium;
>
> (c) introduces or causes to be introduced any virus or other computer contaminant in the Central Identities Data Repository;
>
> (d) damages or causes to be damaged the data in the Central Identities Data Repository;
>
> (e) disrupts or causes disruption of the access to the Central Identities Data Repository;
>
> (f) denies or causes a denial of access to any person who is authorised to access the Central Identities Data Repository;
>
> (g) reveals any information in contravention of sub-section (5) of section 28, or shares, uses or displays information in contravention of section 29 or assists any person in any of the aforementioned acts;
>
> (h) destroys, deletes or alters any information stored in any removable storage media or in the Central Identities Data Repository or diminishes its value or utility or affects it injuriously by any means; or
>
> (i) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used by the Authority with an intention to cause damage,
>
> shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to a fine which shall not be less than ten lakh rupees."

Section 39 imposes a penalty for tampering with data in the CIDR. Sections 40 and 41 impose penalties on requesting and enrolment agencies in case they act in contravention of the obligations imposed upon them under the Act. Section 42 provides for a general penalty for an offence under the Act or the rules or regulations made thereunder, for which no specific penalty is provided under the Act. Under Section 43, when an offence has been committed by a company, every person who at the time the offence was committed was in charge of, and was responsible to the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. Section 44 indicates that the provisions of the Act would apply to any offence or contravention committed outside India by any person, irrespective of nationality. The power to investigate offences under the Act has been placed, under Section 45, on a police officer not below the rank of Inspector of Police.

Section 47(1) of the Act puts a bar on the courts from taking cognizance of any offence punishable under the Act, except when a complaint is made by UIDAI or any officer or person authorised by it. The provision indicates that the scope of cognizance is limited. It does not allow an individual who finds that there is any violation under the Act, to initiate criminal proceedings. The scope of grievance redressal under the Act is restrictive and works only on the action of UIDAI or a person authorised by it. UIDAI has set up a grievance redressal mechanism as contemplated by Section 23(2)(s) of the Aadhaar Act. There is

no grievance redressal mechanism if any breach or offence is committed by UIDAI itself. The right of an individual to seek remedy under the Act if his/her rights are violated will be discussed subsequently. Under sub-Section (2), no court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate can try any offence punishable under the Act.

Section 48 empowers the Central Government to supersede UIDAI, in certain situations. Under Section 50, UIDAI, in exercise of its powers or performance of its functions under the Act, shall be bound by the written directions on questions of policy of the Central Government. Section 51 vests power in UIDAI to delegate to any member, officer or any other person, its powers and functions under the Act (except the power under section 54) as it may deem necessary. Section 51 grants a wide discretion to the UIDAI to delegate any of its powers and functions.

Section 55 requires every rule and regulation made under the Aadhaar Act to be laid down before each House of Parliament. The Section states:

> "55. Laying of rules and regulations before Parliament.-
>
> Every rule and every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation, or both the Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that

> any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation."

UIDAI needs to place the regulations framed by it before Parliament.

53 The architecture of Aadhaar is integral to the exercise of analyzing the reasonableness of the entire project. Whether the architecture addresses the concerns raised by the petitioners is an essential component of this exercise. The architecture of Aadhaar must pass the constitutional requirements of reasonableness and proportionality. This aspect will be dealt under the heading of "proportionality" in a subsequent part of this judgment.

E Passage of Aadhaar Act as a Money Bill

54 The petitioners challenge the constitutionality of the Aadhaar Act, contending that it could not have been passed as a Money Bill. According to the submission, the Aadhaar Act did not qualify as a Money Bill under Article 110 of the Constitution, and it legislates on matters which fall outside that provision. The Attorney General for India submitted that the Constitution accords finality to the decision of the Speaker as to whether a Bill is a Money Bill and hence the question whether the Aadhaar Act fulfils the requirements of being categorized as Money Bill is not open to judicial review. The Attorney General also urged that the Aadhaar Act does fall under Article 110.

Article 110 provides thus:

> "(1) For the purposes of this Chapter, a Bill shall be deemed to be a Money Bill if it contains only provisions dealing with all or any of the following matters, namely:—
> (a) the imposition, abolition, remission, alteration or regulation of any tax;
> (b) the regulation of the borrowing of money or the giving of any guarantee by the Government of India, or the amendment of the law with respect to any financial obligations undertaken or to be undertaken by the Government of India;
> (c) the custody of the Consolidated Fund or the Contingency Fund of India, the payment of moneys into or the withdrawal of moneys from any such Fund;
> (d) the appropriation of moneys out of the Consolidated Fund of India;
> (e) the declaring of any expenditure to be expenditure charged on the Consolidated Fund of India or the increasing of the amount of any such expenditure;
> (f) the receipt of money on account of the Consolidated Fund of India or the public account of India or the custody or issue of such money or the audit of the accounts of the Union or of a State; or
> (g) any matter incidental to any of the matters specified in sub-clauses (a) to (f).
> (2) A Bill shall not be deemed to be a Money Bill by reason only that it provides for the imposition of fines or other pecuniary penalties, or for the demand or payment of fees for licences or fees for services rendered, or by reason that it provides for the imposition, abolition, remission, alteration or regulation of any tax by any local authority or body for local purposes.
> (3) If any question arises whether a Bill is a Money Bill or not, the decision of the Speaker of the House of the People thereon shall be final.
> (4) There shall be endorsed on every Money Bill when it is transmitted to the Council of States under article 109, and when it is presented to the President for assent under article 111, the certificate of the Speaker of the House of the People signed by him that it is a Money Bill."

55 The key questions before this Court are:

(i) Whether under Article 110(3), the decision of the Speaker of the Lok Sabha, that a Bill is a Money Bill, is immune from judicial review;

(ii) If the answer to (i) is in the negative, whether the Aadhaar Act is a Money Bill under Article 110(1) of the Constitution; and

(iii) If the Bill to enact the Aadhaar Act was not a Money Bill, whether a declaration of unconstitutionality will result from its legislative passage as a Money Bill in the Lok Sabha.

E.I Judicial Review of the Speaker's Decision

56 Article 109 provides for a special procedure in respect of Money Bills. It provides that a Money Bill shall not be introduced in the Council of States, the Rajya Sabha. After a Money Bill is introduced in the Lok Sabha and passed by it, the Bill has to be transmitted to the Rajya Sabha for its recommendations. Article 110(4) provides that when a 'Money Bill' is transmitted from the Lower House to the Upper House, it must be endorsed with a certificate by the Speaker of the Lower House that it is a Money Bill. From the date of the receipt of the Money Bill, the Rajya Sabha is bound to return the Bill to the Lok Sabha, within a period of fourteen days, with its recommendations. The Lok Sabha has the discretion to "either accept or reject all or any of the recommendations" made by the Rajya Sabha.[67] If the Lok Sabha accepts any of the recommendations of the Rajya Sabha, the Money Bill is deemed to have been passed by both Houses of the Parliament "with the amendments recommended" by the Rajya Sabha and accepted by the Lok Sabha.[68]

[67] Article 109(2), The Constitution of India
[68] Article 109(3), The Constitution of India

However, when the Lok Sabha "does not accept any of the recommendations" of the Rajya Sabha, the Money Bill is said to have been passed by both Houses in the form in which it was originally passed by the Lok Sabha.[69] If a Money Bill after being passed by the Lok Sabha and transmitted to the Rajya Sabha for its recommendations is not returned to the Lok Sabha within a period of fourteen days, it is then deemed to have been passed by both the Houses of the Parliament in the form in which it was originally passed by the Lok Sabha.[70] When a Money Bill has been passed by the Houses of the Parliament, Article 111 requires it to be presented to the President along with the Lok Sabha Speaker's certificate for assent[71]. Article 117(1) also provides that a Bill "making provision for any of the matters specified in sub-clauses (a) to (f) of clause (1) of article 110" shall also not be introduced in the Rajya Sabha.

57 The Constitution contains corresponding provisions for Money Bills introduced in and passed by a state legislative assembly. Article 198 provides a special procedure for Money Bills in the state legislative assembly. Article 199(3) provides for the finality of the decision of the Speaker of the Legislative Assembly. Under Article 200, when a Money Bill has been passed by the State Legislature, it is to be presented to the Governor, along with the Speaker's certificate, for assent.[72]

[69] Article 109(4), The Constitution of India
[70] Article 109(5), The Constitution of India
[71] Article 110(4), The Constitution of India
[72] Article 199(4), The Constitution of India

Article 107 contains provisions for the introduction and passing of Bills in general and provides thus:

> "(1) Subject to the provisions of articles 109 and 117 with respect to Money Bills and other financial Bills, a Bill may originate in either House of Parliament.
> **(2) Subject to the provisions of articles 108 and 109, a Bill shall not be deemed to have been passed by the Houses of Parliament unless it has been agreed to by both Houses, either without amendment or with such amendments only as are agreed to by both Houses.**
> (3) A Bill pending in Parliament shall not lapse by reason of the prorogation of the Houses.
> (4) A Bill pending in the Council of States which has not been passed by the House of the People shall not lapse on a dissolution of the House of the People.
> (5) A Bill which is pending in the House of the People, or which having been passed by the House of the People is pending in the Council of States, shall, subject to the provisions of article 108, lapse on a dissolution of the House of the People."

58 Ordinary bills can be passed only when they are agreed to by both Houses. Amendments suggested by one House have to be agreed upon by both the Houses for the bill to be passed. Both Houses of Parliament have a vital role assigned by the Constitution in the passage of ordinary bills. Deviating from the important role which it assigns to the Rajya Sabha in the passage of legislation, the Constitution carves out a limited role for the Rajya Sabha in the passage of Money Bills.

59 The Constitution confers special powers on the Speaker of the Lok Sabha in the passage of a Money Bill. Ordinary bills (other than Money Bills) can originate in either House of Parliament. They can be scrutinised, debated in and amended in both the Houses of Parliament during the course of

passage. A Bill is not regarded as being passed by Parliament until both the Houses agree to its passage without amendments or with the amendments as proposed. A constitutional discretion is conferred on the Speaker of the Lok Sabha to decide whether a Bill is a Money Bill. When the Speaker of the Lok Sabha declares a Bill to be a Money Bill, the Rajya Sabha is left only with the option to make recommendations to the Bill within the deadline of fourteen days. Being only recommendations, they do not bind the Lok Sabha. They may either be accepted or rejected by the Lok Sabha.

60 The Rajya Sabha is a constitutional body in a bicameral legislature. The makers of the Constitution adopted bicameralism from Britain. The origin of the limited role that the Upper House has in the passing of a Money Bill can be traced to the British Parliament Act, 1911, which will be discussed in a subsequent part of this analysis. The draftspersons of the Constitution were conscious of the impact of a misuse of institutional power. They provided for a detailed blue print of the architecture of constitutional governance. It is necessary to understand our constitutional history in order to comprehend the scope of the finality attributed to the Speaker's decision on whether or not a Bill is a Money Bill.

61 The origins of the procedure of passing Money Bills in the United Kingdom are older than the Parliament Act of 1911. The authoritative

treatise[73], by Thomas Erskine May, on the law, privileges, proceedings and usage of Parliament in Britain dwells on the history of the evolution of the relationship between the House of Commons and the House of Lords with regard to their powers of taxation and in relation to national revenue and public expenditure.[74]

A grant imposed by the House of Commons would become law in effect, only after the assent of the House of Lords and of the Queen.[75] While the House of Commons enjoyed the legal right to originate grants for nearly 300 years, the House of Lords was originally not precluded from amending a Bill. But in 1671[76] and 1678[77] respectively, the Commons passed two resolutions to curtail the powers of the House of Lords so that only the Commons had the sole right to direct or limit the scope of a Bill regarding taxation and government expenditure. The House of Lords was excluded from altering any such Bill.

The exclusion of the Lords was so strictly followed that the Commons even denied to the former, the power of authorising the taking of fees, imposing

[73] Thomas Erskine May, A treatise on the law, privileges, proceedings and usage of Parliament, Ninth Edition (1883)

[74] Ibid, at pages 637-638. It notes: “At length, when the Commons had increased in political influence, and the subsidies voted by them had become the principal source of national revenue, they gradually assumed their present position in regard to taxation and supply, and included the Lords as well as themselves in their grants. So far back as 1407, it was stated by King Henry IV, in the ordinance called “The Indemnity of the Lords and Commons”, that grants were “granted by the Commons, and assented to by the Lords”.”

[75] Ibid, at page 638

[76] Ibid, at page 641. The Resolution stated: “That in all aids given to the king by the Commons, the rate or tax ought not to be altered”.

[77] Ibid. The Resolution stated: “That all aids and supplies, and aids to his Majesty in Parliament, are the sole gift of the Commons ; and all bills for the granting of any such aids and supplies ought to begin with the Commons : and that it is the undoubted and sole right of the Commons to direct, limit, and appoint in such bills the ends, purposes, considerations, conditions, limitations, and qualifications of such grants ; which ought not to be changed or altered by the House of Lords.”

pecuniary penalties or of varying the mode of suing for them, or of applying them when recovered, though such provisions were necessary to give effect to the general enactments of a Bill.[78] Since this strict enforcement was found to be "attended with unnecessary inconvenience", it led to the adopting of a Standing Order in 1849 which accommodated space to the House of Lords for suggesting amendments on legislative issues.[79] However, the constitutional skirmishes continued. They eventually led to the passage of the Parliament Act of 1911, which essentially deprived the House of Lords of the right to reject Money Bills.

62 The Parliament Act 1911 was explicitly aimed at "regulating the relations between the two Houses of Parliament"[80]. The Preamble of the Act indicates that it was enacted for "restricting the existing powers of the House of Lords"[81]. Section 1(1) provides for the power of the House of Lords on Money Bills:

> "If a Money Bill, having been passed by the House of Commons, and sent up to the House of Lords at least one month before the end of the session, is not passed by the House of Lords without amendment within one month after it is so sent up to that House, the Bill shall, unless the House of Commons direct to the contrary, be present to His Majesty and become an Act of Parliament on the Royal Assent being signified, notwithstanding that the House of Lords have not consented to the Bill."

"Money Bill" was defined statutorily for the first time. Section 1(2) provided:

[78] Ibid, at pages 642-643
[79] Ibid, pages 646-647
[80] Preamble of the Parliament Act 1911
[81] Ibid

> "A Money Bill means a Public Bill which in the opinion of the Speaker of the House of Commons contains only provisions dealing with all or any of the following subjects, namely, the imposition, repeal, remission, alteration, or regulation of taxation; the imposition for the payment of debt or other financial purposes of charges on the Consolidated Fund, [the National Loans Fund] or on money provided by Parliament, or the variation or repeal of any such charges; supply; the appropriation, receipt, custody, issue or audit of accounts of public money; the raising or guarantee of any loan or the repayment thereof; or subordinate matters incidental to those subjects or any of them. In this subsection the expressions "taxation", "public money", and "loan" respectively do not include any taxation, money, or loan raised by local authorities or bodies for local purposes."

The use of the expression "means" in the definition of a Money Bill indicates it was exhaustively defined. A Bill would be a Money Bill, if the Speaker of the House of Commons opined that it contains "only" certain specific provisions. Under Section 1(3), when a Money Bill is sent up to the House of Lords and to Her Majesty for assent, it should be endorsed by a certificate of the Speaker of the House of Commons that it is a Money Bill. This sub-section also provides that before giving his certificate, the Speaker may consult "two members to be appointed from the Chairman's Panel at the beginning of each Session by the Committee of Selection". Therefore, the Speaker has to certify any bill which in his or her opinion falls within the definition of a Money Bill. Any bill containing provisions outside the definition would not be certified as a Money Bill. The Speaker does not certify a Bill until it has reached the form in which it will leave the House of Commons, that is, at the end of its Commons

stage. The Speaker can only decide whether or not to certify a Bill once it has passed the House.[82]

Section 3 of the 1911 Act provides finality to the certificate issued by the Speaker and renders it immune from judicial review. According to it:

> "Any certificate of the Speaker of the House of Commons given under this Act **shall be conclusive for all purposes**, and **shall not be questioned in any court of law.**"
> (Emphasis supplied)

The Act provides finality to the decision of the Speaker of the House of Commons. By using the phrase "shall not be questioned in any court of law", the Act grants immunity to the Speaker's decision from judicial review.

The statutory concept of a 'Money Bill' and the Speaker's certification of a Bill as a 'Money Bill' introduced by the Parliament Act, 1911 ultimately found its way into the Constitution of India, but with significant modifications.

63 In India, the categorization of Money Bills can be said to have begun from the Commonwealth of India Bill 1925, which was drafted by a National Convention comprised of 250 members, with Tej Bahadur Sapru as its Chairman. Article 36 of the Commonwealth Bill provided:

> "36. (a) Any Bill which appropriates revenue or moneys for the ordinary annual services of the Government shall deal only with such appropriation.

[82] House of Lords, Select Committee on the Constitution, Money Bills and Commons Financial Privilege (2011), available at https://publications.parliament.uk/pa/ld201011/ldselect/ldconst/97/97.pdf

> (b) Bills imposing taxation· shall deal only with the imposition of taxes, and any provision therein dealing with any other matter shall be of no effect.
> (c) Bills for the appropriation of revenues or moneys or imposing taxation shall be introduced only by a member of the Cabinet, and can only originate in the Legislative Assembly."

The Bill neither provided a definition of a Money Bill nor did it discuss the role of the Speaker of the Assembly of elected representatives.

In its Madras session of December 1927, the Indian National Congress, as a response to the setting up of the Simon Commission (which did not have any Indian members) decided to set up an All Parties' Conference to draft a Constitution for India. With Motilal Nehru as the Chairman of the Committee constituted by the All Parties' Conference, a Report was prepared. Article 17 of the Nehru Report provided a definition of a Money Bill:

> "17. A money bill means a bill which contains only provisions dealing with all or any of the following subjects, namely the imposition, repeal, remission, alteration or regulation of taxation; the imposition, for the payment of debt or other financial purposes, of charges on public revenues or monies, or the variation or repeal of any such charges; the supply, appropriation, receipt, custody, issue or audit of accounts of public money; the raising of any loan or the repayment thereof; or subordinate matters incidental to those subjects or any of them. In this definition the expression "taxation", "public money" and "loan" respectively do not include any taxation, money or loan raised by local authorities or bodies for local purposes."

The definition of a Money Bill in the Nehru Report, was drawn from the Parliament Act, 1911 in Britain. Article 18 of the Report provided that the "question whether a bill is or is not a money bill will be decided by the

president of the House of Representatives". The House of Representatives (the Lower House) was provided the final authority to either accept or reject the recommendations made by the Senate (the Upper House). Article 19 of the Report provided thus:

> "A money bill passed by the House of Representatives shall be sent to the Senate for its recommendations and it shall be returned not later than… days therefrom to the House of Representatives, which may pass it, accepting or rejecting all or any of the recommendations of the Senate; and the bill so passed shall be deemed to have been passed by both chambers."

While the Constituent Assembly of India was in session, the Socialist Party of India came up with a "Draft Constitution of the Republic of India", based on its ideologies. Article 147 of its Draft Constitution provided:

> "147. (1) A Bill making provision-
> (a) for imposing, abolishing, remitting, altering or regulating any tax ; or
> (b) for regulating the borrowing of money, or giving any guarantee by the Government, or for amending the law with respect to any financial obligations undertaken or to be undertaken by the Government; or
> (c) for declaring any expenditure to be expenditure charged on the public revenues, or for increasing the amount of any such expenditure
> shall be deemed as a money Bill and shall not be introduced or moved except on the recommendation of the Government.
> (2) A Bill or amendment shall not be deemed to make provision for any of the purposes aforesaid by reason only that it provides for the Imposition of fines or other pecuniary penalties, or for the demand and payment of fees for licenses or fees for services rendered, or by reason that it provides for the imposition, abolition, remission, alteration, or regulation of tax by any local authority or body for local purposes.
> (3) In case of dispute whether a Bill is a money Bill or not, the decision of the Speaker, or in his absence of the Deputy Speaker, shall be final."

The Draft Constitution of the Socialist Party conferred a discretion on the Speaker of the Lower House, and in his absence, on the Deputy Speaker, to decide whether a Bill is a Money Bill.

64 There was another model present before the makers of the Indian Constitution. British India was governed by the provisions of the Government of India Act, 1935, which provided for two Houses of Parliament – the Council of States (Upper House) and Federal Assembly (Lower House). Section 37 of the Government of India Act 1935 made special provisions for financial bills:

> "37.-(1) A Bill or amendment making provision- (a) for imposing or increasing any tax; or (b) for regulating the borrowing of money or the giving of any guarantee by the Federal Government, or for amending the law with respect to any financial obligations undertaken or to be undertaken by the Federal Government ; or (c) for declaring any expenditure to be expenditure charged on the revenues of the Federation, or for increasing the amount of any such expenditure, shall not be introduced or moved except on the recommendation of the Governor-General, and a Bill making such provision shall not be introduced in the Council of State."

Under the 1935 Act, there was no provision for a Speaker's certificate regarding a Financial Bill. Section 38(1) authorized each House to make rules regulating its procedure and for the conduct of its business, subject to the provisions of the Act.

A Financial Bill could be introduced only "on the recommendation of the Governor-General". Section 41 provided a general immunity from judicial review on the "ground of any alleged irregularity of procedure":

> "41(1). The validity of any proceedings in the Federal Legislature shall not be called in question on the ground of any alleged irregularity of procedure.
> (2) No officer or other member of the Legislature in whom powers are vested by or under this Act for regulating procedure or the conduct of business, or for maintaining order, in the Legislature shall be subject to the jurisdiction of any court in respect of the exercise by him of those powers."

The Constituent Assembly evidently had these legislative precedents relating to Money Bills which it would have considered while formulating its drafts.

65 While the proceedings of the Constituent Assembly were in motion, Sir B N Rau, as its constitutional advisor, prepared a memorandum of the Draft Constitution for the Union Constitution Committee. It envisaged a Parliament of the Union consisting of the President and two Houses—the Senate and the House of Representatives.[83] One of the proposals discussed in the meetings of the Union Constitution Committee was that "Money Bills would originate in the House of the People and the power of the other House would be limited to making suggestions for amendment, which the House of the People could accept or reject".[84] B Shiva Rao has recorded what transpired during the course of the proceedings of the Constituent Assembly:

> "The Draft also included provisions regarding legislative procedure, procedure in financial matters and general procedure for the conduct of business. No Bill could be submitted for the President's assent unless it had been passed in identical form by both Houses. Except in the case of Money Bills, both Houses enjoyed equal powers; and difference between the two Houses were to be settled by a majority vote in a joint sitting of both Houses convened by the President… Money Bills were defined in the Draft as

[83] B Shiva Rao, The Framing of India's Constitution: A Study, Indian Institution of Public Administration (1968), at page 420
[84] Ibid

> comprising Bills proposing the imposition or increase of any tax, regulating the borrowing of money by the Government of India or the giving of financial guarantees, or declaring any item of expenditure as ‘‘charged” on the revenues, i.e. placing it outside the vote of the House of the People. The general principle approved by the Constituent Assembly was that financial control over the executive would' be - exercised by the House of the People. Accordingly the Draft provided that Money Bills could originate only in that House. The powers of the Council of States in the case of Money Bills were restricted to making suggestions for amendment. If these suggestions were, not accepted by the House of the People, or if the Council of States did not return a Bill within thirty days with its suggestions for amendment, the Bill would be ‘deemed to have been' passed by both Houses in the form in which it was passed' by the House of the People” and submitted to the President for his assent’.”[85]

66 The draft prepared by the Constitutional Advisor provided a definition of a Money Bill, which was inspired by Section 37 of the Government of India Act 1935, Section 53 of the Commonwealth of Australia Constitution Act 1900[86] and Article 22 of the Constitution of Ireland 1937.[87] Article 75 of this draft of the Constitution provided that “if any question arises whether a Bill is a ‘money bill’ or not, the decision of the Speaker of the House of the People thereon shall be final.”[88] Neither Section 37 of the Government of India Act 1935 nor Section 53 of the Commonwealth of Australia Constitution Act 1900

[85] Ibid, at pages 427-428

[86] The said provision provides: “Powers of the Houses in respect of legislation**.**
Proposed laws appropriating revenue or moneys, or imposing taxation, shall not originate in the Senate. But a proposed law shall not be taken to appropriate revenue or moneys, or to impose taxation, by reason only of its containing provisions for the imposition or appropriation of fines or other pecuniary penalties, or for the demand or payment or appropriation of fees for licences, or fees for services under the proposed law. The Senate may not amend proposed laws imposing taxation, or proposed laws appropriating revenue or moneys for the ordinary annual services of the Government. The Senate may not amend any proposed law so as to increase any proposed charge or burden on the people. The Senate may at any stage return to the House of Representatives any proposed law which the Senate may not amend, requesting, by message, the omission or amendment of any items or provisions therein. And the House of Representatives may, if it thinks fit, make any of such omissions or amendments, with or without modifications. Except as provided in this section, the Senate shall have equal power with the House of Representatives in respect of all proposed laws.”

[87] B Shiva Rao, The Framing of India’s Constitution: Selected Documents, Indian Institution of Public Administration (2012), at page 32, as quoted in Pratik Datta, Shefali Malhotra & Shivangi Tyagi, Judicial Review and Money Bills, NUJS Law Review (2017)

[88] Ibid

has a similar provision which accords legal finality to the decision of the Speaker. The draft provision was similar to Article 22 of the Constitution of Ireland 1937, which provides:

> "1. **The Chairman of Dáil Éireann[89] shall certify any Bill which, in his opinion, is a Money Bill to be a Money Bill, and his certificate shall, subject to the subsequent provisions of this section, be final and conclusive**.
> 2. Seanad Éireann[90], by a resolution, passed at a sitting at which not less than thirty members are present, may request the President to refer the question whether the Bill is or is not a Money Bill to a Committee of Privileges.
> 3. If the President after consultation with the Council of State decides to accede to the request he shall appoint a Committee of Privileges consisting of an equal number of members of Dáil Éireann and of Seanad Éireann and a Chairman who shall be a Judge of the Supreme Court: these appointments shall be made after consultation with the Council of State. In the case of an equality of votes but not otherwise the Chairman shall be entitled to vote.
> 4. The President shall refer the question to the Committee of Privileges so appointed and the Committee shall report its decision thereon to the President within twenty-one days after the day on which the Bill was sent to Seanad Éireann.
> 5. The decision of the Committee shall be final and conclusive.
> 6. If the President after consultation with the Council of State decides not to accede to the request of Seanad Éireann, or if the Committee of Privileges fails to report within the time hereinbefore specified the certificate of the Chairman of Dáil Éireann shall stand confirmed." (Emphasis supplied)

67 The draft prepared by the Advisor to the Constituent Assembly did not adopt the above provision in its entirety. It adopted the part on the finality of the certification of the Speaker on whether a Bill is a Money Bill. The Irish model of dispute resolution, which provided for a mechanism to review the Speaker's certification, was not adopted.

[89] Lower House in Ireland
[90] Upper House in Ireland

Subsequently, in its report submitted to the President of the Constituent Assembly on 5 December 1947, the Expert Committee on Financial Provisions suggested an amendment to the draft provision, to the effect that:

> "When a Money Bill is sent from the Lower House to the Upper, a certificate of the Speaker of the Lower House saying that it is a Money Bill should be attached to, or endorsed on, the bill and a provision to that effect should be made in the Constitution on the lines of the corresponding provision in the Parliament Act, 1911. **This will prevent controversies about the matter outside the Lower House.**"[91] (Emphasis supplied)

Certification of any Bill by the Speaker of the Lower House as a Money Bill, was envisaged for procedural simplicity to avoid causing confusion in the Upper House of Parliament.

68 The final provision which has assumed the form of Article 110 of the Constitution, does not contain the exact language used in the Act of 1911. The 1911 Act of the British Parliament consciously excluded judicial review of the certificate of the Speaker of the House of Commons. The intention of the British Parliament is clear from the specific language used in Section 3 of the Act. Section 3 accords finality to the decision of the Speaker by providing that any certificate of the Speaker of the House of Commons "shall be conclusive for all purposes, and shall not be questioned in any court of law". The certification of the Speaker is both conclusive and immune from judicial review. The framers of the Indian Constitution did not adopt this language.

[91] B Shiva Rao, The Framing of India's Constitution: Selected Documents, Indian Institution of Public Administration, at page 281

Rather, they chose to adopt the phrase “shall be final”. The phrase used in the Act of 1911 expressly excluded courts from exercising their power of judicial review over the decision of the Speaker of the House of Commons. This language was used in the 1911 Act to put an end to the constitutional skirmishes experienced by the House of Lords and the House of Commons in Britain for more than five hundred years, leading to the enactment of the 1911 Act.[92] The deviation from incorporating the language, used in the 1911 Act, into the Indian Constitution is reflective of the intention of our Constitution makers that they did not want to confer the same status on the power assigned to the Speaker of the Lok Sabha, as is provided to the Speaker of the House of Commons. Had their intention been otherwise, they would have used the same language as that provided under the 1911 Act. Finality would operate as between the Houses of Parliament. It did not exclude judicial review by a constitutional Court.

69 The British legal system adopts the principle of parliamentary sovereignty. That is not so in India. Ours is a system founded on the supremacy of the Constitution. Judicial review is an essential component of constitutional supremacy. A Constitution Bench of this Court in **Kalpana Mehta** v **Union of India**[93] has, while noticing this distinction, held:

> “…The fundamental difference between the two systems lies in the fact that parliamentary sovereignty in the Westminster form of government in the UK has given way, in the Indian Constitution, to constitutional supremacy. Constitutional

[92] Pratik Datta, Shefali Malhotra & Shivangi Tyagi, Judicial Review and Money Bills, NUJS Law Review (2017)
[93] (2018) 7 SCC 1

> supremacy mandates that every institution of governance is subject to the norms embodied in the constitutional text. The Constitution does not allow for the existence of absolute power in the institutions which it creates. Judicial review as a part of the basic features of the Constitution is intended to ensure that every institution acts within its bounds and limits."[94]

70 The purpose of judicial review is to ensure that constitutional principles prevail in interpretation and governance. Institutions created by the Constitution are subject to its norms. No constitutional institution wields absolute power. No immunity has been attached to the certificate of the Speaker of the Lok Sabha from judicial review, for this reason. The Constitution makers have envisaged a role for the judiciary as the expounder of the Constitution. The provisions relating to the judiciary, particularly those regarding the power of judicial review, were framed, as Granville Austin observed, with "idealism"[95]. Courts of the country are expected to function as guardians of the Constitution and its values. Constitutional courts have been entrusted with the duty to scrutinize the exercise of power by public functionaries under the Constitution. No individual holding an institutional office created by the Constitution can act contrary to constitutional parameters. Judicial review protects the principles and the spirit of the Constitution. Judicial review is intended as a check against arbitrary conduct of individuals holding constitutional posts. It holds public functionaries accountable to constitutional duties. If our Constitution has to survive the vicissitudes of political aggrandisement and to face up to the prevailing

[94] Ibid, at para 227
[95] Granville Austin, The Indian Constitution: Cornerstone of a Nation, Oxford University Press (1966), at page 205

cynicism about all constitutional institutions, notions of power and authority must give way to duties and compliance with the rule of law. Constitutional institutions cannot be seen as focal points for the accumulation of power and privilege. They are held in trust by all those who occupy them for the moment. The impermanence of power is a sombre reflection for those who occupy constitutional offices. The Constitution does not contemplate a debasement of the institutions which it creates. The office of the Speaker of the House of People, can be no exception. The decision of the Speaker of the Lok Sabha in certifying a Bill as a Money Bill is liable to be tested upon the touchstone of its compliance with constitutional principles. Nor can such a decision of the Speaker take leave of constitutional morality.

71 Our Constitution does not provide absolute power to any institution. It sets the limits for each institution. Our constitutional scheme envisages a system of checks and balances. The power of the Speaker of the Lok Sabha, to decide whether a Bill is a Money Bill, cannot be untrammelled. The contention that the decision of Speaker is immune from judicial review and cannot be questioned, is contrary to the entire scheme of the Constitution, which is premised on transparency, non-arbitrariness and fairness. The phrase “shall be final” used in Article 110(3) has been adopted, as mentioned earlier, from Article 22 of the Irish Constitution. The provisions of Article 22 of the Irish Constitution provide a mechanism for review of the certificate issued by the Speaker. Recourse is provided under the Irish Constitution by which

the members of the Upper House of the Irish Parliament can request the President of Ireland to refer the question of whether a Bill is a Money Bill, to a Committee of Privileges. If the President refers the question to this Committee, the decision of the Committee stands “final and conclusive”. The members of the Constituent Assembly did not adopt this mechanism. Absence of this mechanism does not mean that the decision of the Speaker of the Lok Sabha cannot be subject to checks and balances, of which judicial review is an indispensable facet. The Speaker has to act within the domain, which the Constitution accords to the office of the Speaker. The power conferred on the Speaker of the Lok Sabha cannot be exercised arbitrarily, for it could damage the scheme of the Constitution. Judicial review is the ultimate remedy to ensure that the Speaker does not act beyond constitutional entrustment.

72 The scope of the phrase “shall be final” can also be understood by looking at the proceedings of the Constituent Assembly. The constitutional foundation of Article 110(4) is based upon a suggestion of the Expert Committee on Financial Provisions that when a Money Bill is transmitted from the Lower House to the Upper House, it should be endorsed by the Speaker’s certificate, so as to prevent any controversy “about the matter outside the Lower House”. Therefore, the finality provided to the decision of the Speaker as to whether a Bill is a Money Bill or not, is aimed at avoiding any controversy on the issue in the Rajya Sabha and before the President. Had it been intended to prevent the court from adjudicating upon the validity of the

decision of the Speaker, the language of the Article would have made it explicit. Where a constitutional provision evinces a specific intent to exclude judicial review, clear words to that effect are used. Articles 243O(a)[96], 243ZG(a)[97] and 329(a) specifically use the phrase – "shall not be called in question in any court". For instance, Article 329(a) provides thus:

> "Notwithstanding anything in this Constitution —
> (a) the validity of any law relating to the delimitation of constituencies or the allotment of seats to such constituencies, made or purporting to be made under article 327 or article 328, **shall not be called in question in any court**." (Emphasis supplied)

73 In **N P Ponnuswami** v **Returning Officer, Namakkal Constituency, Namakkal, Salem District**[98], a six judge Bench of this Court, while construing the provisions of Article 329, compared it to the preceding Articles, and held thus:

> "5…A notable difference in the language used in articles 327 and 328 on the one hand, and article 329 on the other, is that while the first two articles begin with the words "subject to the provisions of this Constitution", the last article begins with the words "notwithstanding anything in this Constitution". It was conceded at the Bar that the effect of this difference in language is that whereas any law made by Parliament under article 327, or by the State Legislature under article 328, cannot exclude the jurisdiction of the High Court under article 226 of the Constitution, that jurisdiction is excluded in regard to matters provided for in article 329."[99]

[96] Article 243O(a), which is a part of the chapter on Panchayats, provides: "Notwithstanding anything in this Constitution,— (a) the validity of any law relating to the delimitation of constituencies or the allotment of seats to such constituencies, made or purporting to be made under article 243K, shall not be called in question in any court."

[97] Article 243ZG(a), which is a part of the chapter on Municipalities, provides: "Notwithstanding anything in this Constitution,— (a) the validity of any law relating to the delimitation of constituencies or the allotment of seats to such constituencies, made or purporting to be made under article 243ZA shall not be called in question in any court."

[98] 1952 SCR 218

[99] Ibid, at para 5

74 In order to understand the scope of the finality attached to the Speaker's decision under Article 110(3), it would be useful to analyse how in the case of other constitutional provisions, the words "shall be final" have been interpreted by this Court. Articles 217(3)[100], 311(3)[101] and paragraph 6(1) of the Tenth Schedule[102] contain the phrase "shall be final". In **Union of India** v **Jyoti Prakash Mitter**[103], this Court held that it can examine the legality of an order passed by the President on the determination of the age of a Judge of the High Court under Article 217 (3) of the Constitution. The six judge Bench held:

> "32…The President acting under Article 217(3) performs a judicial function of grave importance under the scheme of our Constitution. He cannot act on the advice of his Ministers. Notwithstanding the declared finality of the order of the President the Court has jurisdiction in appropriate cases to set aside the order, if it appears that it was passed on collateral considerations or the rules of natural justice were not observed, or that the President's judgment was coloured by the advice or representation made by the executive or it was founded on no evidence…Appreciation of evidence is entirely left to the President and it is not for the Courts to hold that on the evidence placed before the President on which the conclusion is founded, if they were called upon to decide the case they would have reached some other conclusion."[104]

The President was held to perform a judicial function in making a determination under Article 217(3).

---

[100] Article 217 (3) states: "If any question arises as to the age of a Judge of a High Court, the question shall be decided by the President after consultation with the Chief Justice of India and the decision of the President shall be final."

[101] Article 311(3) states: "If, in respect of any such person as aforesaid, a question arises whether it is reasonably practicable to hold such inquiry as is referred to in clause (2), the decision thereon of the authority empowered to dismiss or remove such person or to reduce him in rank shall be final."

[102] Paragraph 6(1) states "If any question arises as to whether a member of a House has become subject to disqualification under this Schedule, the question shall be referred for the decision of the Chairman, or, as the case may be, the Speaker of such House and his decision shall be final:
Provided that where the question which has arisen is as to whether the Chairman or the Speaker of a House has become subject to such disqualification, the question shall be referred for the decision of such member of the House as the House may elect in this behalf and his decision shall be final."

[103] (1971) 1 SCC 396

[104] Ibid, at page 397

The question of finality under Article 311(3) was dealt with by a Constitution Bench of this Court in **Union of India** v **Tulsiram Patel**[105]. The Court held that the finality given to the decision of the disciplinary authority by Article 311(3) that it is not reasonably practicable to hold an enquiry, is not binding upon the Court so far as its power of judicial review is concerned.

The constitutional validity of the provisions contained in the Tenth Schedule to the Constitution came up for consideration before a Constitution Bench of this Court in **Kihoto Hollohan** v **Zachillhu**[106]. The Constitution Bench held that the power vested in the Speaker or the Chairman under the Schedule, is a judicial power, and was amenable to judicial review:

> "111…That Paragraph 6(1) of the Tenth Schedule, to the extent it seeks to impart finality to the decision of the Speakers/Chairmen is valid. **But the concept of statutory finality embodied in Paragraph 6(1) does not detract from or abrogate judicial review under Articles 136, 226 and 227 of the Constitution in so far as infirmities based on violations of constitutional mandates, mala fides, non-compliance with Rules of Natural Justice and perversity, are concerned.**"[107] (Emphasis supplied)

The Bench had also clarified that:

> "101…The principle that is applied by the courts is that in spite of a finality clause it is open to the court to examine whether the action of the authority under challenge is ultra vires the powers conferred on the said authority. Such an action can be ultra vires for the reason that it is in contravention of a mandatory provision of the law conferring on the authority the power to take such an action. It will also be ultra vires the powers conferred on the authority if it is

[105] (1985) 3 SCC 398
[106] (1992) Supp (2) SCC 651
[107] Ibid, at page 711

> vitiated by mala fides or is colourable exercise of power based on extraneous and irrelevant considerations..."[108]

Undoubtedly, the finality clauses contained in Article 217(3), 311(3) and in paragraph 6(1) of the Tenth Schedule were held not to exclude judicial review since the essential nature of the power is judicial. A constitutional function is entrusted to the Speaker to certify a Bill as a Money Bill under Article 110(3), to which the attributes of a judicial power do not apply. Indeed, the power which is entrusted to the Speaker under Article 110(3) is integral to the legislative process. But, the fact that the authority which a constitutional functionary exercises is not of a judicial character, is not sufficient to lead to the conclusion that a finality clause governing the exercise of that power makes it immune from judicial review. Where the entrustment of the power is subject to the due fulfilment of constitutional norms, the exercise of jurisdiction is amenable to judicial review, to the extent necessary to determine whether there has been a violation of a constitutional mandate. The nature and extent of judicial review would undoubtedly vary from a situation where finality has been attached to a judicial, administrative or quasi-judicial power. However, a clause on finality notwithstanding, it is open to the constitutional court to determine as to whether there has been a violation of a constitutional mandate as a result of which the decision suffers from a constitutional infirmity. The entrustment of a constitutional function to the Speaker under Article 110(3) to certify a Bill as a Money Bill is premised on the fulfilment of the norms stipulated in Article 110(1). A certification can be questioned on the ground

[108] Ibid, at page 708

that the Bill did not fulfil the conditions stipulated in Article 110(1) to be designated as a Money Bill. If that is established, the certification would be contrary to constitutional mandate. Whether that is so can be judicially scrutinized.

75 The notion that an entrustment of power is absolute has a colonial origin. Law under a colonial regime was not just an instrument to maintain order but was a source of subordination. Recognition of the vesting of absolute authority was but a reflection of the premise that those who ruled could not be questioned. Those who were ruled had to accept the authority of the ruler. Nothing can be as divorced from constitutional principle as these normative foundations of colonial law and history. The notion that power is absolute is inconsistent with a Constitution which subjects the entrustment of functions to public functionaries to the restraints which accompany it. Our law must recognise the need to liberate its founding principles from its colonial past. The Court should not readily accept the notion that the authority vested in a constitutional functionary is immune from judicial review. In the absence of a specific exclusion of judicial review, none can be implied. Moreover, any exclusion of judicial review must be tested on the anvil of its functionality. A specific exclusion of judicial review, in order to be valid, must serve a constitutional function. The test of functionality must relate to whether an exclusion of review is necessary to fulfil the overarching need for the proper discharge of a constitutional role. Exclusion of review, to be valid, must fulfil

the requirement of a constitutional necessity. Its purpose cannot be to shield an excess of power from being questioned before the Court. Nor is the fact that a power is vested in a high functionary a ground to shield it from scrutiny. The ultimate test is whether the exclusion of judicial review is express and specific and, whether such an exclusion is designed to achieve a constitutional purpose that meets the test of functionality, assessed in terms of a constitutional necessity. In the seventh decade of the republic, our interpretation of the Constitution must subserve the need to liberate it from its colonial detritus.

This approach was adopted by a seven judge Bench of this Court in **Krishna Kumar Singh** v **State of Bihar**[109]. While interpreting the ordinance making power of the Governor, the Court held that the interpretation of the Constitution must be "carefully structured" to ensure that the power remains what the framers of our Constitution intended it to be. The Bench held:

> "91…The issue which needs elaboration is whether an ordinance which by its very nature has a limited life can bring about consequences for the future (in terms of the creation of rights, privileges, liabilities and obligations) which will enure beyond the life of the ordinance. **In deciding this issue, the court must adopt an interpretation which furthers the basic constitutional premise of legislative control over ordinances. The preservation of this constitutional value is necessary for parliamentary democracy to survive on the sure foundation of the Rule of law and collective responsibility of the executive to the legislature. The silences of the Constitution must be imbued with substantive content by infusing them with a meaning which enhances the Rule of law.** To attribute to the executive as an incident of the power to frame ordinances, an unrestricted ability to create binding effects for posterity would

[109] (2017) 3 SCC 1

> set a dangerous precedent in a parliamentary democracy. The court's interpretation of the power to frame ordinances, which originates in the executive arm of government, cannot be oblivious to the basic notion that the primary form of law making power is through the legislature..."[110] (Emphasis supplied)

The ordinance making power was held to be an exceptional power to meet a "constitutional necessity".

76 The marginal note to Article 122 is: "Courts not to inquire into proceedings of Parliament". The Article reads thus:

> "122. (1) The validity of any proceedings in Parliament shall not be called in question on the ground of any alleged irregularity of procedure.
> (2) No officer or member of Parliament in whom powers are vested by or under this Constitution for regulating procedure or the conduct of business, or for maintaining order, in Parliament shall be subject to the jurisdiction of any court in respect of the exercise by him of those powers."

This Court must deal with the question whether the Speaker's decision under Article 110(3) is protected by Article 122. Article 122 prohibits courts from examining the validity of any proceedings in Parliament on the ground that there was "any alleged irregularity of procedure". The content of the expression "procedure" referred to in the Article, is indicated in Article 118 of the Constitution. The marginal note to Article 118 provides for "Rules of procedure". Article 118 provides as follows:

> "118. (1) Each House of Parliament may make **rules for regulating, subject to the provisions of this Constitution, its procedure and the conduct of its business**.
> (2) Until rules are made under clause (1), the rules of

[110] Ibid, at pages 76-77

> procedure and standing orders in force immediately before the commencement of this Constitution with respect to the Legislature of the Dominion of India shall have effect in relation to Parliament subject to such modifications and adaptations as may be made therein by the Chairman of the Council of States or the Speaker of the House of the People, as the case may be.
> (3) The President, after consultation with the Chairman of the Council of States and the Speaker of the House of the People, may make rules as to the procedure with respect to joint sittings of, and communications between, the two Houses.
> (4) At a joint sitting of the two Houses the Speaker of the House of the People, or in his absence such person as may be determined by rules of procedure made under clause (3), shall preside." (Emphasis supplied)

77 Articles 118 to 122 are covered under the rubric of the general heading- "Procedure Generally". Article 118 provides for rules to be made by each House of Parliament for regulating the procedure and conduct of its business. The Article subjects these contemplated rules to the provisions of the Constitution. The provision does not indicate that these rules will stand above the Constitution. They are, on the contrary, subject to the Constitution. The rules framed under Article 118, are procedural in nature. The procedure contemplated under Articles 118 to 122 is distinct from substantive constitutional requirements. The obligation placed on the Speaker of the Lok Sabha to certify whether a Bill is a Money Bill is not a mere matter of "procedure" contemplated under Article 122. It is a constitutional requirement, which has to be fulfilled according to the norms set out in Article 110. Article 122 will not save the action of the Speaker, if it is contrary to constitutional norms provided under Article 110. The Court, in the exercise of its power of judicial review, can adjudicate upon the validity of the action of the Speaker if

it causes constitutional infirmities. Article 122 does not envisage exemption from judicial review, if there has been a constitutional infirmity. The Constitution does not endorse a complete prohibition of judicial review under Article 122. It is only limited to an "irregularity of procedure".

78 This Court has on several occasions restricted the scope of the bar provided under Article 122 (and under corresponding Article 212 for the States) and has distinguished an "irregularity of procedure" from "illegality". In **Special Reference No. 1 of 1964**[111], a seven judge Bench of this Court brought home that distinction in the context of Article 212(1) with the following observations:

> "61…Article 212(2) confers immunity on the officers and members of the Legislature in whom powers are vested by or under the Constitution for regulating procedure or the conduct of business, or for maintaining order, in the Legislature from being subject to the jurisdiction of any court in respect of the exercise by him of those powers. Art. 212(1) seems to make it possible for a citizen to call in question in the appropriate court of law the validity of any proceedings inside the legislative chamber if his case is that the said proceedings suffer **not from mere irregularity of procedure, but from an illegality. If the impugned procedure is illegal and unconstitutional, it would be open to be scrutinised in a court of law, though such scrutiny is prohibited if the complaint against the procedure is no more than this that the procedure was irregular...**" (Emphasis supplied)

In **Ramdas Athawale** v **Union of India**[112] **("Ramdas Athawale")**, a Constitution Bench of this Court extended the above formulation to Article 122 of the Constitution:

[111] AIR 1965 SC 745
[112] (2010) 4 SCC 1

> "36.This Court *Under Article 143, Constitution of India, In re (Special Reference No. 1 of 1964)* [AIR 1965 SC 745 : (1965) 1 SCR 413] (also known as Keshav Singh case [AIR 1965 SC 745 : (1965) 1 SCR 413]) while construing Article 212(1) observed that it may be possible for a citizen to call in question in the appropriate Court of law, the validity of any proceedings inside the Legislature if his case is that the said proceedings suffer not from mere irregularity of procedure, but from an illegality. If the impugned procedure is illegal and unconstitutional, it would be open to be scrutinized in a Court of law, though such scrutiny is prohibited if the complaint against the procedure is no more than this that the procedure was irregular. The same principle would equally be applicable in the matter of interpretation of Article 122 of the Constitution."[113]

A Constitution Bench of this Court reaffirmed the distinction between a "procedural irregularity" and an "illegality" in **Raja Ram Pal** v **Hon'ble Speaker, Lok Sabha**[114] **("Raja Ram Pal")**. The Bench held that courts are not prohibited from exercising their power of judicial review to examine any illegality or unconstitutionality in the procedure of Parliament:

> "386…Any attempt to read a limitation into Article 122 so as to restrict the court's jurisdiction to examination of the Parliament's procedure in case of unconstitutionality, as opposed to illegality would amount to doing violence to the constitutional text. Applying the principle of "expressio unius est exclusio alterius" (whatever has not been included has by implication been excluded), **it is plain and clear that prohibition against examination on the touchstone of "irregularity of procedure" does not make taboo judicial review on findings of illegality or unconstitutionality**…[115]
>
> 398… the Court will decline to interfere if the grievance brought before it is restricted to allegations of "irregularity of procedure". But in case gross illegality or violation of constitutional provisions is shown, the judicial review will not be inhibited in any manner by Article 122, or for that matter by Article 105."[116]

[113] Ibid, at pages 13-14
[114] (2007) 3 SCC 184
[115] Ibid, at page 359
[116] Ibid, at page 362

The Court distinguished the constitutional background in India from that of England, holding that while England has adopted a regime of exclusive parliamentary dominance, India is governed by a system of checks and balances provided in the Constitution:

> "366.The touchstone upon which Parliamentary actions within the four-walls of the Legislature were examined was both the constitutional as well as substantive law. **The proceedings which may be tainted on account of substantive illegality or unconstitutionality, as opposed to those suffering from mere irregularity thus cannot be held protected from judicial scrutiny by Article 122(1)** in as much as the broad principle laid down in Bradlaugh [(1884) 12 QBD 271] acknowledging **exclusive cognizance of the Legislature in England has no application to the system of governance provided by our Constitution wherein no organ is sovereign and each organ is amenable to constitutional checks and controls, in which scheme of things, this Court is entrusted with the duty to be watchdog of and guarantor of the Constitution.**"[117] (Emphasis supplied)

The principle which emerges from these decisions is that the decision of the Speaker is amenable to judicial review, if it suffers from illegality or from a violation of constitutional provisions.

79 The Attorney General advanced the submission that this Court has on previous occasions refrained from scrutinizing the decision of the Speaker on whether a Bill is a Money Bill. Those decisions require discussion for adjudicating the present case. In **Mangalore Ganesh Beedi Works** v **State of Mysore**[118] **("Mangalore Beedi")**, a new system of coinage was introduced by amending the Indian Coinage Act. Under the new system, while one rupee

[117] Ibid, at page 350
[118] 1963 Supp (1) SCR 275

was divided into a hundred naya paisas, the old legal tender of sixteen annas or sixty four pice remained legal tender equivalent to one hundred naya paisas. The appellant, which was a firm registered under the Mysore Sales Tax Act, had to pay an additional amount as sales tax due to change in the currency. It was argued that by the substitution of 2 naya paisas (the new currency) in place of 3 pies (the old currency) as tax, there was a change in the tax imposed by the Mysore Sales Tax Act, which could only have been done by passing a Money Bill under Articles 198, 199 and 207 of the Constitution and since no Money Bill was introduced or passed for the enhancement of the tax, the tax was illegal and invalid. The contention, therefore, was that the procedure envisaged for passing a Money Bill ought to have been, but was not, followed. The Constitution Bench dismissed the appeal, holding that the substitution of a new coinage i.e. naya paisas in place of annas, pice and pies did not amount to an enhancement of tax. It was held to be merely a substitution of one coinage by another of equivalent value. This Court held that the levy of tax in terms of naya paisas was not unconstitutional nor was it a taxing measure but it dealt merely with the conversion of the old coinage into new coinage. Having held this, the Bench also remarked:

> "5…Even assuming that it is a taxing measure its validity cannot be challenged on the ground that it offends Arts. 197 to 199 and the procedure laid down in Art. 202 of the Constitution. Article 212 prohibits the validity of any proceedings in a legislature of a State from being called in question on the ground of any alleged irregularity of procedure and Art. 255 lays down that requirements as to recommendation and previous sanction are to be regarded as matters of procedure only..."

The Court having found that a substitution of coinage did not result in an enhancement of tax, Article 199 was not attracted. The legislative measure was not a Money Bill. Once that was the case, the subsequent observations (extracted above) proceeded on an assumption: that even if it were a taxing measure, it would be saved by Article 255. The court having held that no enhancement of tax was involved in a mere substitution of coinage, the alternative hypothesis is not a part of the ratio and was unnecessary. The ratio was that substitution of a new coinage did not amount to a Money Bill. The decision of the Constitution Bench in **Mangalore Beedi** dealt with the contention that a Money Bill was unconstitutionally passed as an ordinary Bill. The Bench held that substitution of coinage did not make it a Money Bill. The decision contains a general observation regarding the immunity of proceedings in a state legislature. A scholarly article[119] has correctly referred to the general remarks made in **Mangalore Beedi** as unnecessary and not the ratio since the issue was already decided on merits, by holding that the substitution of coinage was not an enhancement of tax.

80 A three judge Bench of this Court in **Mohd Saeed Siddiqui** v **State of Uttar Pradesh**[120] **("Mohd Saeed Siddiqui")** dealt with the constitutional validity of the Uttar Pradesh Lokayukta and Up-Lokayuktas (Amendment) Act, 2012. Section 5(1) of the unamended Act provided a term of six years for the Lokayukta. Section 5(3) provided that on ceasing to hold office, the Lokayukta

[119] Pratik Datta, Shefali Malhotra & Shivangi Tyagi, Judicial Review and Money Bills, Vol 10, NUJS Law Review (2017).
[120] (2014) 11 SCC 415

or Up-Lokayukta shall be ineligible for further appointment. The new State government, which came in office, introduced a Bill which was passed as the Uttar Pradesh Lokayukta and Up-Lokayuktas (Amendment) Act, 2012, by which the term of the U.P. Lokayukta and Up-Lokayukta was extended from six years to eight years or till the successor enters upon office. The Amendment Act also limited the ineligibility of the Lokayuktas or Up-Lokayuktas for further appointment under the Government of Uttar Pradesh. The Amendment Act was challenged on the ground that it was passed as a Money Bill when, on the face of it, it could never have been called a Money Bill under Article 199 of the Constitution. The Bench rejected the petition holding that the question "whether a Bill is a Money Bill or not can be raised only in the State Legislative Assembly by a member thereof when the Bill is pending in the State Legislature and before it becomes an Act". It relied upon the observations made in **Mangalore Beedi,** to formulate following principles:

> "(i) the validity of an Act cannot be challenged on the ground that it offends Articles 197 to 199 and the procedure laid down in Article 202; (ii) Article 212 prohibits the validity of any proceedings in a Legislature of a State from being called in question on the ground of any alleged irregularity of procedure; and (iii) Article 255 lays down that the requirements as to recommendation and previous sanction are to be regarded as a matter of procedure only. It is further held that the validity of the proceedings inside the Legislature of a State cannot be called in question on the allegation that the procedure laid down by the law has not been strictly followed and that no Court can go into those questions which are within the special jurisdiction of the Legislature itself, which has the power to conduct its own business."

The judgment also made a reference to the seven judge Bench decision in **Pandit MSM Sharma** v **Dr Shree Krishna Sinha**[121] **("MSM Sharma")**.

The "proceedings of the Legislature" were held to include "everything said or done in either House" in the transaction of parliamentary business. Relying upon Articles 212 and 255, the Bench accorded finality to the decision of the Speaker:

> "43. As discussed above, the decision of the Speaker of the Legislative Assembly that the Bill in question was a Money Bill is final and the said decision cannot be disputed nor can the procedure of the State Legislature be questioned by virtue of Article 212. Further, as noted earlier, Article 255 also shows that under the Constitution the matters of procedure do not render invalid an Act to which assent has been given to by the President or the Governor, as the case may be. Inasmuch as the Bill in question was a Money Bill, the contrary contention by the Petitioner against the passing of the said Bill by the Legislative Assembly alone is unacceptable."[122]

Making a passing reference to the decision of the Constitution Bench in **Raja Ram Pal**, the Bench opined that even if it is established that there was some infirmity in the procedure in the enactment of the Amendment Act, it will be protected by Article 255 of the Constitution.

81 Subsequently, a two judge Bench of this Court in **Yogendra Kumar Jaiswal** v **State of Bihar**[123] **("Yogendra Kumar**") dealt with the constitutional validity of the Orissa Special Courts Act, 2006. The law was enacted by the

[121] AIR 1960 SC 1186
[122] Mohd Saeed Siddiqui, Ibid, at page 430
[123] (2016) 3 SCC 183

State legislature, keeping in view the accumulation of properties disproportionate to their known sources of income by persons who have held or hold high political and public offices. The legislature provided special courts for speedy trial of certain classes of offences and for confiscation of properties. The appellants, who were public servants and facing criminal cases, challenged the Act on the ground that it was introduced in the State Assembly as a Money Bill though it did not have any characteristics of a Money Bill under Article 199 of the Constitution. The Court dismissed the petitions, following the decision in **Mohd Saeed Siddiqui**. It held that:

> "43. In our considered opinion, the authorities cited by the learned Counsel for the Appellants do not render much assistance, for the introduction of a bill, as has been held in Mohd. Saeed Siddiqui (supra), comes within the concept of "irregularity" and it does come with the realm of substantiality. What has been held in the Special Reference No. 1 of 1964 (supra) has to be appositely understood. The factual matrix therein was totally different than the case at hand as we find that the present controversy is wholly covered by the pronouncement in Mohd. Saeed Siddiqui (supra) and hence, we unhesitatingly hold that there is no merit in the submission so assiduously urged by the learned Counsel for the Appellants."[124]

Special Reference No. 1 of 1964 was distinguished in **Yogendra Kumar**.

Article 255 provides:

> "No Act of Parliament or of the Legislature of a State, and no provision in any such Act, shall be invalid by reason only that some recommendation or previous sanction required by this Constitution was not given, if assent to that Act was given—
> (a) where the recommendation required was that of the Governor, either by the Governor or by the President;
> (b) where the recommendation required was that of the Rajpramukh, either by the Rajpramukh or by the President;

[124] Ibid, at page 229

> (c) where the recommendation or previous sanction required was that of the President, by the President."

82 Article 255 speaks about a situation where a "recommendation or previous sanction" is required to be given by the Governor, Rajpramukh or, as the case may be, by the President. The absence of a recommendation or previous sanction will not invalidate the law, where the Act has received the assent of the Governor or the President. Subsequent assent, in other words, cures the absence of recommendation or sanction. Article 255 is in no way related to the decision or certificate of the Speaker of the Lok Sabha or of the State Legislative Assembly on whether a Bill is a Money Bill. Moreover, Article 255 does not apply to Articles 110 for the simple reason that the latter does not embody either a previous sanction or recommendation. Article 255 does not envisage superseding the role of the Upper House of Parliament or the State Legislature. **Mohd Saeed Siddiqui** proceeds on an erroneous understanding of Article 255. **Mohd Saeed Siddiqui** was followed in **Yogendra Kumar**. These two judgments cite the same three articles — Articles 199,[125] 212,[126] and 255, to refrain from questioning the conduct of the Speaker, without noticing that Article 255 does not apply there.

Further, **MSM Sharma,** which was referred in **Mohd Saeed Siddiqui** was discussed in the **Special Reference** to hold that the validity of any proceedings in a legislative chamber can be questioned if such proceedings

[125] Corresponding provision for the Union is Article 110 of the Constitution.
[126] Corresponding provision for the Union is Article 122 of the Constitution.

suffer from illegality. The consistent thread which emerges from the judgments in **Special Reference, Ramdas Athawale** and **Raja Ram Pal** is that the validity of proceedings in Parliament or a State Legislature can be subject to judicial review on the ground that there is an illegality or a constitutional violation. Moreover, the judgment in **Yogendra Kumar** followed **Mohd Saeed Siddiqui**. **Siddiqui** was based on an erroneous understanding of **Mangalore Beedi**. The decision of the Speaker under Articles 110(3) and 199(3) is not immune from judicial review.

The three judge Bench decision in **Mohd Saeed Siddiqui** and the two judge Bench decision in **Yogendra Kumar** are overruled.

83 Barring judicial review of the Lok Sabha Speaker's decision would render a certification of a Bill as a Money Bill immune from scrutiny, even where the Bill does not, objectively speaking, deal only with the provisions set out in Article 110(1). The decision of the Speaker of the Lok Sabha whether a Bill is a Money Bill impacts directly upon the constitutional role which will be discharged by the Rajya Sabha in relation to it. The Lok Sabha alone does not represent Parliament. The Indian Parliament is bicameral. The Constitution envisages a special role for the Rajya Sabha. In order to truly understand the relevance of the Rajya Sabha in the Indian context, an analysis of major bicameral systems is necessary, as an exercise in comparative law.

84 Bicameral legislatures are not unique to either the Presidential or Parliamentary forms of government. Democracies with a Presidential form of government have adopted bicameral legislatures, the United States being the leading example. Among Parliamentary democracies, India and the UK have adopted bicameral legislatures. They are predominant in federal countries. Where second chambers exist, they vary in terms of powers and composition. Together, their powers and composition shape the impact that they have on legislation.[127] The phenomenon of the bicameral system has two different historic origins. It was first established in England, and later in the US.[128] Both these models have been replicated across the globe.

85 Britain developed some of the earliest institutional practices that came to be emulated through the Western world. A separate powerful legislature was initiated when King John in 1215 gave a written commitment to seek the consent of Parliament to levy taxes to which he was entitled by feudal prerogative. Over the next five centuries, the British Parliament was transformed from an institution summoned at the desire of the ruler to one which met on regular occasions to develop policy inclinations independent of the wishes of the ruler.[129] In the fourteenth century, Parliament was divided into two chambers: one chamber (the House of Lords) in which debate took place with the feudal lords and a second chamber (the House of Commons)

[127] Fathali M. Moghaddam, The SAGE Encyclopaedia of Political Behaviour (2017).
[128] Betty Drexhage, Bicameral Legislatures: An International Comparison, Ministry of the Interior and Kingdom Relations- Netherlands (2015), at page 7
[129] Abhinay Muthoo & Kenneth A. Shepsle, The Constitutional Choice of Bicameralism, in Institutions and Economic Performance (Elhanan Helpman ed.), Harvard University Press (2008), at pages 251-252

where the citizens were represented.[130] The upper chamber of the British Parliament, the Lords, comprised of hereditary peers (whose number varied with the discretion of the King to create them). The lower chamber, the Commons, represented individuals satisfying a substantial property requirement. The two chambers in Britain reflected a kind of class division. Before the beginning of the eighteenth century, several factors such as civil war, regicide, experimentation with a republic, and the restoration of the titular monarch caused power to be permanently shifted from the King to Parliament.[131]

Around the same time, the British colonies in North America were crafting institutions of their own. Colonial legislatures were being conceptualized on similar lines, with some exceptions, to British Parliament. The Constitution for the newly formed United States adopted a bicameral system.[132] The legislature in the United States was innovative, for it created a bicameral arrangement that replaced a class basis (as was in existence in Britain) for chamber representation with a modified federal basis. The Constitutional Convention of 1787 had provided for a lower chamber, a directly-elected House of Representatives, where each voter had an equal vote in elections, and an upper chamber, a Senate, to which each state could send two members, elected indirectly by the state parliaments. The Convention was a

[130] Betty Drexhage, Bicameral Legislatures: An International Comparison, Ministry of the Interior and Kingdom Relations- Netherlands (2015), at page 7

[131] Abhinay Muthoo & Kenneth A. Shepsle, The Constitutional Choice of Bicameralism, in Institutions and Economic Performance (Elhanan Helpman ed.), Harvard University Press (2008), at page 252

[132] Betty Drexhage, Bicameral Legislatures: An International Comparison, Ministry of the Interior and Kingdom Relations- Netherlands (2015), at page 8

compromise between those who wanted a parliament in which the states, irrespective of their population size, would have an equal voice, and those who wanted a Parliament for the newly formed federal nation where the participating states were represented in proportion to the size of their population. A system with two differently composed chambers was ultimately chosen to be the only way out of the deadlock.[133] The rationale for a bicameral legislature comprising of a directly elected Lower House and an indirectly elected Upper House was best articulated by James Madison, in the *Federalist Papers:*

> "*First*… a senate, as a second branch of the legislative assembly, distinct from, and dividing the power with, a first, must be in all cases a salutary check on the government. It doubles the security to the people, by requiring the concurrence of two distinct bodies in schemes of usurpation or perfidy, where the ambition or corruption of one would otherwise be sufficient…
> *Second*. The necessity of a senate is not less indicated by the propensity of all single and numerous assemblies to yield to the impulse of sudden and violent passions, and to be seduced by factious leaders into intemperate and pernicious resolutions…
> *Third*. Another defect to be supplied by a senate lies in a want of due acquaintance with the objects and principles of legislation. It is not possible that an assembly of men called for the most part from pursuits of a private nature, continued in appointment for a short time, and led by no permanent motive to devote the intervals of public occupation to a study of the laws, the affairs, and the comprehensive interests of their country, should, if left wholly to themselves, escape a variety of important errors in the exercise of their legislative trust… A good government implies two things: first, fidelity to the object of government, which is the happiness of the people; secondly, a knowledge of the means by which that object can be best attained…
> *Fourth*. The mutability in the public councils arising from a rapid succession of new members, however qualified they

[133] Betty Drexhage, Bicameral Legislatures: An International Comparison, Ministry of the Interior and Kingdom Relations- Netherlands (2015), at page 7

> may be, points out, in the strongest manner, the necessity of some stable institution in the government…"[134]

Madison conceptualized that the second chamber would fulfil significant roles: (a) it would provide the certainty that the government will not neglect its obligations to its constituents, as the chamber provides an extra check on it; (b) it can curb the actions of the other chamber if it gives into the urge to follow 'sudden and pronounced sentimental reactions'; (c) it can meet the need for expertise in the framing of laws and the interests of the country, and thus help to avoid legislative mistakes; and (d) it can be a factor for stability that ensures continuity in the administration of the country.

86 Bicameralism, in both systems, emerged as a development associated with the changing conceptions of the state. The literature on bicameralism has highlighted the importance of having a second chamber in the legislature of a state. William Riker has emphasized that a bicameral structure acts as a control over the tyranny of a majority.[135] Levmore similarly echoes this thought:

> "At the very least, if the two chambers consider an issue simultaneously, one chamber's agenda setter will be at the mercy of the order of consideration in the second chamber. Bicameralism can thus be understood as an antidote to the manipulative power of the convenor, or agenda setter, when faced with cycling preferences."[136]

[134] James Madison, The Federalist No. 62 – The Senate, The Federalist Papers (1788), available at http://www.constitution.org/fed/federa62.html

[135] William H. Riker, The Justification of Bicameralism, International Political Science Review (1992), Vol. 13, Issue 1, at pages 101–16.

[136] Saul Levmore, Bicameralism: When Are Two Decisions Better than One?, International Review of Law and Economics (1992), Vol. 12, at pages 147-148.

A study[137] commissioned by the Dutch Ministry of the Interior and Kingdom Relations analysed the design of the bicameral system in several countries. The study consulted constitutional texts and literature on the evolution of bicameralism and came to the finding that:

> "Historically, the creation of bicameral systems, both in the federal and the aristocratic variant, always was a concession to those (states or estates) who risked losing power in the new setting. In emerging democracies, and up until the present day, the choice of a bicameral system appears as a means of dispelling fear about the consequences of democratisation and reconciling established elites with the democratisation process. In developed democracies, the rationale of a bicameral system is now sought primarily in the possibility of combining different systems of representation (particularly in federal systems) and in the possibility of reconsideration by a different chamber in the legislative, making it possible to avoid making mistakes and enhancing both the quality and the stability of the legislation. In majority systems of the Westminster model - where the government is part of the lower house and it tends to have a stable majority - a senate moreover is sometimes ascribed the role of giving more independent input into the parliamentary work, less determined by party discipline, and of paying more attention to the interests of minorities. A bicameral system is, for that reason, sometimes recommended as a means to protect minorities against a tyranny of the majority… Finally, a bicameral system may also increase efficiency because it is possible to divide the legislative workload between two chambers. That can be the case when the two chambers absorb a sort of division of labour (e.g. an emphasis on technical legal quality in the senate). In many bicameral systems, moreover, it can be decided to put bills to either house, and the senate also has a right of initiative."[138]

87 The importance of the second chamber increases when there is no single party rule in Parliament. Governments that lack Upper-House majority

[137] Betty Drexhage, Bicameral Legislatures: An International Comparison, Ministry of the Interior and Kingdom Relations- Netherlands (2015).
[138] Ibid, at pages 11-12

support find it difficult to pass Bills.[139] Elliot Bulmer notes pertinently that in a democracy, a second chamber addresses the inability of the elected chamber to adequately represent a diverse society. In this view, a second chamber may enable a "more nuanced and complete representation of society, with greater representation for territorial, communal or other minorities".[140]

While discussing the advantage of second chambers in republican legislatures, Rogers observes that the institution of a second chamber generates legislative advantage only "if the chambers differ significantly from one another".[141] Quoting from the work of various scholars, he observes:

> "Hammond and Miller find that "The stability-inducing properties of bicameralism are . . . dependent on the existence of distinctly different viewpoints in the two chambers"… Buchanan and Tullock conclude similarly that, "unless the bases for representation are significantly different in the two houses, there would seem to be little excuse for the two-house system"… Because two "congruent" chambers would ostensibly not significantly affect policy outcomes, Lijphart described bicameral systems with congruent chambers as "weak" forms of bicameralism…"[142]

88 Bicameralism, when entrenched as a principle in a constitutional democracy, acts as a check against the abuse of power by constitutional means or its use in an oppressive manner. As a subset of the constitutional principle of division of power, bicameralism is mainly a safeguard against the abuse of the constitutional and political process. A bicameral national

[139] James N. Druckman & Michael F. Thies, The Importance of Concurrence: The Impact of Bicameralism on Government Formation and Duration, American Journal of Political Science (2002), Vol. 46, No. 4, at pages 760-771.
[140] Elliot Bulmer, Bicameralism, International Institute for Democracy and Electoral Assistance (2017), at page 4
[141] James R. Rogers, The Advantage of Second Chambers in Republican Legislatures: An Informational Theory, at page 6, available at https://ecpr.eu/Filestore/PaperProposal/beb20221-c2c5-4475-9b9f-74bb3f1512a7.pdf
[142] Ibid

parliament can hold the government accountable and can check or restrain the misuse of government power. Among its other roles is that of representing local state units, acting as a body of expert review, and providing representation for diverse socio-economic interests or ethno-cultural minorities.

While deliberating over the necessity of having a second chamber, the Constituent Assembly had the benefit of examining the constitutional history of several other nations. The constitutional advisor, B N Rau, found the issue of second chambers to be “one of the most vexing questions of political science”.[143] Under colonial rule, bicameralism had already been introduced. The first bicameral legislature as the national assembly for India was established by the Government of India Act 1919. The Government of India Act, 1935 had created an Upper House in the federal legislature which consisted of members elected by the provincial legislatures as well as representatives sent by numerous princely states that were not under the direct control of the British government. The 1935 Act became the blueprint for the structure of Parliament in the new Constitution. The Rajya Sabha, as the Upper House of the Parliament, was adopted into the Constitution. The vision of the Constitution makers behind the establishment of the Upper House of Parliament has found expression in the classic work of Granville Austin:

[143] Granville Austin, The Indian Constitution: Cornerstone of a Nation, Oxford University Press (1966), at page 195

> "The members of the Constituent Assembly had one predominant aim when framing the Legislative provisions of the Constitution: to create a basis for the social and political unity of the country… The goals of the Constituent Assembly… were to bring popular opinion into the halls of government, and, by the method of bringing it there, to show Indians that although they were many peoples, they were but one nation."[144]

89 Article 80 of the Constitution deals with the composition of the Rajya Sabha. The maximum strength of this chamber is 250 members, out of which up to 238 members are elected representatives from the states and union territories. 12 members are nominated by the President among persons with a special knowledge or practical experience in literature, science, art and social service. Members representing the states are elected by the state legislatures through proportional representation by means of a single transferable vote[145]. The method of electing representatives from Union territories has been left to prescription by Parliament.[146] In a departure from the American model of equal representation for the states, the allocation of seats in the Rajya Sabha to the States and Union territories is in accordance with the division provided in the Fourth Schedule of the Constitution (read with Articles 4(1) and 80(2)). The reason behind this division of seats is "to safeguard the interests of the smaller states while at the same time ensuring the adequate representation of the larger states, so that the will of the representatives of a minority of the electorate does not prevail over that of

[144] Granville Austin, The Indian Constitution: Cornerstone of a Nation, Oxford University Press (1966), at pages 180 & 203
[145] Article 80(4), The Constitution of India
[146] Article 80(5), The Constitution of India

those who represented the majority"[147]. In this sense, the Rajya Sabha has a special structure.

90 The institutional structure of the Rajya Sabha has been developed to reflect the pluralism of the nation and its diversity of language, culture, perception and interest. The Rajya Sabha was envisaged by the makers of the Constitution to ensure a wider scrutiny of legislative proposals. As a second chamber of Parliament, it acts as a check on hasty and ill-conceived legislation, providing an opportunity for scrutiny of legislative business. The role of the Rajya Sabha is intrinsic to ensuring executive accountability and to preserving a balance of power. The Upper Chamber complements the working of the Lower Chamber in many ways. The Rajya Sabha acts as an institution of balance in relation to the Lok Sabha and represents the federal structure[148] of India. Both the existence and the role of the Rajya Sabha constitute a part of the basic structure of the Constitution. The architecture of our Constitution envisions the Rajya Sabha as an institution of federal bicameralism and not just as a part of a simple bicameral legislature. Its nomenclature as the 'Council of States' rather than the 'Senate' appropriately justifies its federal importance.[149] Seervai has observed that the federal principle is dominant in our Constitution. While adverting to several of its

[147] Sidharth Chauhan, Bicameralism: comparative insights and lessons, Seminar (February, 2013) available at http://india-seminar.com/2013/642/642_sidharth_chauhan.html

[148] In SR Bommai v Union of India (AIR 1994 SC 1998), a seven-judge Bench of this Court held: "Democracy and federalism are the essential features of our Constitution and are part of its basic structure."

[149] Rajya Sabha Secretariat, Second Chamber In Indian Parliament: Role and Status of Rajya Sabha, (2009), at page 2. See also M.N. Kaul and S.L. Shakdher, Practice and Procedure of Parliament, Lok Sabha Secretariat (2001)

federal features, Seervai emphasises the position of the Rajya Sabha as an integral element:

> "First and foremost, Parliament (the Central Legislature) is dependent upon the States, because one of its Houses, the Council of States, is elected by the Legislative Assemblies of the States. Where the ruling party, or group of parties, in the House of the People has a majority but not an overwhelming majority, the Council of States can have a very important voice in the passage of legislation other than financial Bills. Secondly, a Bill to amend the Constitution requires to be passed by each House of Parliament separately by an absolute majority in that House and by not less than two-thirds of those present and voting. Since the Council of States is indirectly elected by the State Legislatures, the State Legislatures have an important say in the amendment of the Constitution because of the requirement of special majorities in each House. Thirdly, the very important matters mentioned in the proviso to Article 368 (Amendment of the Constitution) cannot be amended unless the amendments passed by Parliament are ratified by not less than half the number of Legislatures of the States… Fourthly, the amendment of Article 352 by the 44th Amendment gives the Council of States a most important voice in the declaration of Emergency, because a proclamation of emergency must be approved by *each House* separately by majorities required for an amendment of the Constitution… Fifthly, the executive power of the Union is vested in the President of India who is not directly elected by the people but is elected by an electoral college consisting of (a) the elected members of the Legislative Assemblies of the States and (b) the elected members of both Houses of Parliament… Directly the State Legislatures have substantial voting power in electing the President; that power is increased indirectly through the Council of States, which is elected by the Legislative Assemblies of States."[150]

91 The Rajya Sabha represents the constituent states of India. It legitimately holds itself as the guardian of the interest of the component states in a federal polity. It endeavours to remain concerned and sensitive to the aspirations of the states, thereby strengthening the country's "federal fabric"

[150] H M Seervai, Constitutional Law of India, Universal Law Co. Pvt. Ltd, Vol. 1, (1991), at pages 299-300.

and "promotes national integration".[151] Being the federal chamber of Parliament, the Rajya Sabha enjoys some special powers, which are not even available to the Lok Sabha, under the Constitution[152]:

> "(i) Article 249 of the Constitution provides that Rajya Sabha may pass a resolution, by a majority of not less than two-thirds of the Members present and voting to the effect that it is necessary or expedient in the national interest that Parliament should make a law with respect to any matter enumerated in the State List. Then, Parliament is empowered to make a law on the subject specified in the resolution for the whole or any part of the territory of India. Such a resolution remains in force for a maximum period of one year but this period can be extended by one year at a time by passing a further resolution;
> (ii) Under Article 312 of the Constitution, if Rajya Sabha passes a resolution by a majority of not less than two-thirds of the Members present and voting declaring that it is necessary or expedient in the national interest to create one or more All India Services common to the Union and the States, Parliament has the power to create by law such services; and
> (iii) Under the Constitution, President is empowered to issue Proclamations in the event of national emergency (Article 352), in the event of failure of constitutional machinery in a State (Article 356), or in the case of financial emergency (Article 360). Normally, every such Proclamation has to be approved by both Houses of Parliament within a stipulated period. Under certain circumstances, however, Rajya Sabha enjoys special powers in this regard. If a Proclamation is issued at a time when the dissolution of the Lok Sabha takes place within the period allowed for its approval, then the Proclamation can remain effective if a resolution approving it, is passed by Rajya Sabha."

92 The Rajya Sabha is a permanent body as it is not subject to dissolution.[153] Being an indirectly elected House, it has no role in the making or unmaking of the Government and therefore it is comparatively "free from

[151] Rajya Sabha Secretariat, Second Chamber In Indian Parliament: Role and Status of Rajya Sabha, (2009), at page 6.
[152] Rajya Sabha Secretariat, Structure and Functions of Rajya Sabha Secretariat, (2009), at pages 2-3
[153] Under Article 83(1), the Rajya Sabha is a permanent body with members being elected for 6 year terms and one-third of the members retiring every 2 years.

compulsions of competitive party politics".[154] As a revising chamber, the Constitution makers envisioned that it will protect the values of the Constitution, even if it is against the popular will. The Rajya Sabha is a symbol against majoritarianism.

A Constitution Bench of this Court in **Kuldip Nayar** v **Union of India**[155] highlighted the importance of the Rajya Sabha:

> "47. The Rajya Sabha is a forum to which experienced public figures get access without going through the din and bustle of a general election which is inevitable in the case of Lok Sabha. It acts as a revising chamber over the Lok Sabha. The existence of two debating chambers means that all proposals and programmes of the Government are discussed twice. As a revising chamber, the Rajya Sabha helps in improving Bills passed by the Lok Sabha..."[156]

93 Participatory governance is the essence of democracy. It ensures responsiveness and transparency. An analysis of the Bills revised by the Rajya Sabha reveals that in a number of cases, the changes recommended by the Rajya Sabha in the Bills passed by the Lok Sabha were eventually carried out.[157] The Dowry Prohibition Bill is an example of a legislation in which the Rajya Sabha's insistence on amendments led to the convening of a joint sitting[158] of the two Houses and in that sitting, one of the amendments

[154] Rajya Sabha Secretariat, Second Chamber In Indian Parliament: Role and Status of Rajya Sabha, (2009), at pages 7-8
[155] (2006) 7 SCC 1
[156] Ibid, at page 47
[157] Rajya Sabha Secretariat, Second Chamber In Indian Parliament: Role and Status of Rajya Sabha, (2009), at page 5
[158] Dr Ambedkar explained that the joint sitting had been kept at the centre because of the federal character of the Central Legislature. See Granville Austin, The Indian Constitution: Cornerstone of a Nation, Oxford University Press (1966), at page 202

suggested by the Rajya Sabha was adopted without a division.[159] The Rajya Sabha has a vital responsibility in nation building, as the dialogue between the two houses of Parliament helps to address disputes from divergent perspectives. The bicameral nature of Indian Parliament is integral to the working of the federal Constitution. It lays down the foundations of our democracy. That it forms a part of the basic structure of the Constitution, is hence based on constitutional principle. The decision of the Speaker on whether a Bill is a Money Bill is not a matter of procedure. It directly impacts on the role of the Rajya Sabha and, therefore, on the working of the federal polity.

94 There is a constitutional trust which attaches to the empowerment of the Speaker of the Lok Sabha to decide whether a legislative measure is a Money Bill. Entrustment of the authority to decide is founded on the expectation that the Speaker of the Lok Sabha will not dilute the existence of a co-ordinate institution in a bicameral legislature. A constitutional trust has been vested in the office of the Speaker of the Lok Sabha. By declaring an ordinary Bill to be a Money Bill, the Speaker limits the role of the Rajya Sabha. This power cannot be unbridled or bereft of judicial scrutiny. If the power of the Speaker is exercised contrary to constitutional norms, it will not only limit the role of the Rajya Sabha, but denude the efficacy of a legislative body created by the Constitution. Such an outcome would be inconsistent

[159] Rajya Sabha Secretariat, Second Chamber In Indian Parliament: Role and Status of Rajya Sabha, (2009), at page 5

with the scheme of the Indian Constitution. Judicial review is necessary to ensure that the federal features of the Constitution are not transgressed.

E.2 Aadhaar Act as a Money Bill

This Court must now deal with whether the Aadhaar Act was validly passed as a Money Bill.

95 Article 110(1) of the Constitution defines a Money Bill. For a Bill to be a Money Bill, it must contain “only provisions” dealing with every or any one of the matters set out in sub-clauses (a) to (g) of clause 1 of Article 110. The expression “if it contains only provisions dealing with all or any of the following matters, namely...” is crucial. Firstly, the expression “if” indicates a condition and it is only upon the condition being fulfilled that the deeming fiction of a Bill being a Money Bill for the purposes of the Chapter will arise. Secondly, to be a Money Bill, the Bill should have only those provisions which are referable to clauses (a) to (g). The condition is much more stringent than stipulating that the Bill should incorporate any of the matters spelt out in clauses (a) to (g). The words “only provisions” means that besides the matters in sub clauses (a) to (g), the Bill shall not include anything else. Otherwise, the expression “only” will have no meaning. The word “only” cannot be treated to be otiose or redundant. Thirdly, the two expressions “if it contains only provisions” and “namely” indicate that sub-clauses (a) to (g) are exhaustive of what a Money Bill may contain. The contents of a Money Bill have to be confined to all or any

of the matters specified in sub-clauses (a) to (g). Fourthly, sub-clause (g) covers any matter incidental to sub-clauses (a) to (f). A matter is incidental when it is ancillary to what is already specified. Sub-clause (g) is not a residuary entry which covers all other matters other than those specified in sub-clauses (a) to (f). If sub-clause (g) were read as a catch-all residuary provision, it would defeat the purpose of defining a class of Bills as Money Bills. What is incidental under sub-clause (g) is that which is ancillary to a matter which is already specified in sub-clauses (a) to (f). The test is not whether it is incidental to the content of a Bill but whether it is incidental to any of the matters specifically enumerated in sub-clauses (a) to (f). The Attorney General would request the court to read the word “only” before “if” and not where it occurs. If the submission were to be accepted, it would lead to the consequence that the Bill would be a Money Bill if it contained provisions dealing with clause (a) to (g), even if it contained other provisions not relatable to these clauses. We cannot rewrite the Constitution, particularly where it is contrary to both text, context and intent.

Clause (2) of Article 110 provides that a Bill shall not be deemed to be a Money Bill just for the reason that it provides for the imposition of fines or other pecuniary penalties, or for the demand or payment of fees for licences or fees for services rendered, or by reason that it provides for the imposition, abolition, remission, alteration or regulation of any tax by any local authority or body for local purposes. Like in the Parliament Act of 1911, the definition of a

Money Bill provided under Article 110(1) is exhaustive in nature. A Bill can be a Money Bill if it contains "only provisions" dealing with all or any of the matters listed under sub-clauses (a) to (g) of Article 110(1).

96 A Financial Bill is different from a Money Bill. Article 117 provides for special provisions relating to Financial Bills. Clause (1) of Article 117 states:

> "(1) A Bill or amendment making provision for any of the matters specified in sub-clauses (a) to (f) of clause (1) of article 110 shall not be introduced or moved except on the recommendation of the President and a Bill making such provision shall not be introduced in the Council of States."

A Financial Bill does not need to have "only provisions" dealing with Sub-clauses (a) to (f) of Article 110. The provisions of Article 110(1) are therefore narrow and exhaustive.

97 As a matter of interpretation, the use of the word "only" indicates that a particular entry is exhaustive and is inapplicable to anything which falls outside its scope. This Court has interpreted the expression "only" as a word of exclusion and restriction.[160] The interpretation of Article 110(1) as being restrictive in nature is also supported by the proceedings in the Constituent Assembly of India. Article 110 corresponds to Article 90 of the Draft Constitution. On 20 May 1949, a member of the Constituent Assembly, Ghanshyam Singh Gupta, proposed an amendment in clause (1) of Article 90

[160] Hari Ram v. Baby Gokul Prasad, (1991) Supp (2) SCC 608; M/s Saru Smelting (P) Ltd. v. Commissioner of Sales Tax, Lucknow, (1993) Supp (3) SCC 97.

to delete the word “only”. He stated that a Bill can be a Money bill even while containing other provisions. Gupta argued:

> “This article is a prototype of Section 37 of the Government of India Act which says that a Bill or amendment providing for imposing or increasing a tax or borrowing money, etc. shall not be introduced or moved except on the recommendation of the Governor-General. This means that the whole Bill need not be a money Bill: it may contain other provisions, but if there is any provision about taxation or borrowing, etc. It will come under this Section 37, and the recommendation of the Governor-General is necessary. Now **article 90 says that a Bill shall be deemed to be a money Bill if it contains only provisions dealing with the imposition, regulation, etc., of any tax or the borrowing of money, etc. This can mean that if there is a Bill which has other provisions and also a provision about taxation or borrowing etc., it will not become a money Bill. If that is the intention I have nothing to say; but that if that is not the intention I must say the word "only" is dangerous, because if the Bill does all these things and at the same time does something else also it will not be a money Bill.** I do not know what the intention of the Drafting Committee is but I think this aspect of the article should be borne in mind.”[161] (Emphasis supplied)

Another member Naziruddin Ahmad also emphasized on the deletion of the word “only”. The concern of these two members was that the word “only” restricts the scope of a Bill being passed as a Money Bill. Their apprehension was that if a Bill has other provisions which are unrelated to the clauses mentioned in draft Article 90, the Bill would not qualify to be a Money Bill in view of the word “only”. The amendment suggested by these members was listed to be put to vote on a later date. The amendment was rejected when it was put to vote on 8 June 1949. The framers of the Indian Constitution consciously rejected the said amendment.

[161] Constituent Assembly Debates (20 May 1949)

98 When a Bill is listed as a Money Bill, it takes away the power of the Rajya Sabha to reject or amend the Bill. The Rajya Sabha can only make suggestions to a Money Bill, which are not binding on the Lok Sabha. The Constitution makers would have been aware about the repercussions of a Bill being introduced as a Money Bill. As the role of the Rajya Sabha is limited in the context of Money Bills, the scope of what constitutes a Money Bill was restricted by adopting the word “only” in Draft Article 90. A Bill to be a Money Bill must not contain any provision which falls outside clauses (a) to (g) of Article 110(1). The Constitution has carefully used the expression “dealing with” in Article 110 (1) and not the wider legislative form “related to”. A Bill, which has both – certain provisions which fall within sub-clauses (a) to (g) of Article 110(1) and other provisions which fall outside will not qualify to be a Money Bill. It is for this reason that there cannot also be any issue of the severability of the provisions of a Bill, which has certain provisions relating to sub-clauses (a) to (g) of Article 110(1), while also containing provisions which fall beyond. Any other interpretation would result in rewriting the Constitution. If a Bill contains provisions which fall outside sub-clauses (a) to (g), it is not a Money Bill. The Rajya Sabha is entitled as part of its constitutional function to legislative participation. The entirety of the Bill cannot be regarded as a Money Bill, once it contains any matters which fall beyond sub-clauses (a) to (g). Once that is the position, it could be impossible to sever those parts which fall within sub-clauses (a) to (g) and those that lie outside. The presence of matters which travel beyond sub-clauses (a) to (g) has consequences in terms

of the nature of the Bill and the legislative participation of the Rajya Sabha. If the constitutional function of the Rajya Sabha has been denuded on the hypothesis that this Bill was a Money Bill, the consequence of a finding in judicial review that the Bill is not a Money Bill must follow. Any other construction will reduce bicameralism to an illusion.

This interpretation is also supported by the judgment of a Bench of seven judges of this Court in **Krishna Kumar Singh** v **State of Bihar**[162], where it held that the ordinance making power conferred upon the President and the Governors is limited by the requirements set out by Articles 123 and 213. This Court had held:

> "59…The constitutional conferment of a power to frame ordinances is in deviation of the normal mode of legislation which takes place through the elected bodies comprising of Parliament and the state legislatures. Such a deviation is permitted by the Constitution to enable the President and Governors to enact ordinances which have the force and effect of law simply because of the existence of circumstances which can brook no delay in the formulation of legislation. In a parliamentary democracy, the government is responsible collectively to the elected legislature. The subsistence of a government depends on the continued confidence of the legislature. **The ordinance making power is subject to the control of the legislature over the executive. The accountability of the executive to the legislature is symbolised by the manner in which the Constitution has subjected the ordinance making power to legislative authority. This, the Constitution achieves by the requirements of Article 213**..."[163] (Emphasis supplied)

99 The authority of the Lok Sabha to pass a Money Bill is based on the requirements set out under Article 110. The framers of the Indian Constitution

[162] (2017) 3 SCC 1
[163] Ibid, at page 61

deliberately restricted the scope of Article 110(1) to ensure that the provision is not an avenue to supersede the authority of the Rajya Sabha. The intention of the Constitution makers is clear. The Lok Sabha cannot introduce and pass a legislative measure in the garb of a Money Bill, which could otherwise have been amended or rejected by the Rajya Sabha. Bicameralism is a founding value of our democracy. It is a part of the basic structure of the Constitution. Introduction and passing of a Bill as a Money Bill, which does not qualify to be a Money Bill under Article 110(1) of the Constitution, is plainly unconstitutional. The Lok Sabha is not entrusted with the entire authority of Parliament. The Lok Sabha, the Rajya Sabha and the President together constitute the Parliament of India. The Lok Sabha is a body of elected representatives and represents the aspirations of citizens. Yet, like every constitutional institution, it is part of this basic structure of the Constitution. A political party or a coalition which holds the majority in the Lok Sabha cannot subvert the working of the Constitution, against which Dr B R Ambedkar had warned[164] in the Constituent Assembly. A ruling government has to work within constitutional parameters and has to abide by constitutional morality.

100 The Constitution of India is not a mere parchment of paper. It was written with the vision of those who gave blood and sweat to freedom: political personalities, social reformers and constitution framers. It symbolises a faith in institutions, justice and good governance. That vision cannot be belied. The

[164] Constituent Assembly Debates (4 November, 1948). Dr Ambedkar had remarked: "… it is perfectly possible to pervert the Constitution, without changing its form by merely changing the form of the administration and to make it inconsistent and opposed to the spirit of the Constitution."

Speaker of the Lok Sabha has an onerous constitutional duty to ensure that a Bill, which is not a Money Bill is not passed as a Money Bill. The Speaker of the Lok Sabha, the Chairman of the Rajya Sabha, the members of the Lok Sabha and the Rajya Sabha, and the President need to work in constitutional solidarity to ensure that no provision of the Constitution is diluted or subverted.

101 The Aadhaar Act was passed as a Money Bill. The provisions of the Act need to be analysed to determine whether the Act is a Money Bill.

The Preamble of the Act states that it is:

> "An Act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto."

The Preamble focuses on the delivery of subsidies, benefits and services for which the expenditure is borne from the Consolidated Fund of India. But the essential issue is whether the Act confines itself to matters which fall within the ambit of Article 110.

102 Section 3 entitles every resident[165] in India to obtain an Aadhaar number by submitting his or her demographic information, by undergoing the process of enrolment. Section 2(m) defines "enrolment" as the process to

[165] Section 2(v) provides: "resident" means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment.

collect demographic and biometric information from individuals by the enrolling agencies for the purpose of issuing Aadhaar numbers to such individuals. After receiving the demographic and biometric information of the individual, the Unique Identification Authority of India (UIDAI) would verify the information and shall issue an Aadhaar number to such an individual.[166] Section 4(3) provides that the Aadhaar number may be accepted as proof of identity for "any purpose". Section 5 requires UIDAI to take special measures to issue Aadhaar numbers to "women, children, senior citizens, persons with disability, unskilled and unorganised workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and such other categories of individuals". Under Section 6, UIDAI may require Aadhaar number holders to update their demographic information and biometric information, from time to time so as to ensure continued accuracy of their information in the Central Identities Data Repository ("CIDR"). The Aadhaar Act defines CIDR as a centralised database containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other related information.[167]

103 Section 7 requires proof of an Aadhaar number as a necessary condition to avail subsidies, benefits and services, for which the expenditure is borne from the Consolidated Fund of India. The proviso to Section 7 states that if an Aadhaar number is not assigned to an individual, the individual shall

[166] Section 3(3), Aadhaar Act
[167] Section 2(h), Aadhaar Act

be offered alternate and viable means of identification for delivery of the subsidy, benefit or service. Section 8(1) requires UIDAI to perform authentication[168] of the Aadhaar number of an Aadhaar number holder, in relation to his or her biometric information or demographic information submitted by any requesting entity[169]. Under Section 8(2), a requesting entity is required to obtain the consent of an individual before collecting his or her identity information for the purposes of authentication. The requesting entity must ensure that the identity information of an individual collected by it is only used for submission to the CIDR for authentication. Section 8(3) requires a requesting entity to inform the individual submitting identity information for authentication certain details with respect to authentication.

104 Chapter IV of the Act deals with UIDAI. Section 11 establishes UIDAI as the body responsible for the processes of enrolment and authentication and for performing functions assigned to it under the Act. The Act provides for the composition of UIDAI[170], qualifications of its members[171], terms of office[172] of its chairperson and members, their removal[173] and functions[174]. Section 23, which deals with the powers and functions of UIDAI, authorizes it to develop the policy, procedure and systems for issuing Aadhaar numbers to individuals

[168] Section 2(c) provides: "authentication" means the process by which the Aadhaar number alongwith demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.
[169] Section 2 (u) provides: "requesting entity" means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication
[170] Section 12, Aadhaar Act
[171] Section 13, Aadhaar Act
[172] Section 14, Aadhaar Act
[173] Section 15, Aadhaar Act
[174] Section 17, Aadhaar Act

and to perform authentication. Section 23(h) states that UIDAI has the power to specify the "manner of use of Aadhaar numbers" for the purposes of providing or availing of various subsidies, benefits, services and "other purposes" for which Aadhaar numbers may be used. Under Section 23(3), UIDAI may enter into a Memorandum of Understanding or agreement with the Central Government or State Governments or Union territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing, securing or processing of information or delivery of Aadhaar numbers to individuals or performing authentication.

105 Chapter V deals with grants, accounts and audit and annual reports of UIDAI. Section 25 provides that the fees or revenue collected by UIDAI shall be credited to the Consolidated Fund of India. Chapter VI deals with protection of information collected from individuals for authentication. Section 28(3) requires UIDAI to take all necessary measures to ensure that the information in its possession or control, including information stored in the CIDR, is secured and protected against access, use or disclosure (not permitted under the Act or the regulations), and against accidental or intentional destruction, loss or damage. Section 29 imposes restrictions on sharing of core biometric information, collected or created under the Act. Section 32(2) entitles every Aadhaar number holder to obtain his or her authentication record in such manner as may be specified by regulations. Section 33 provides for disclosure of information pursuant to a court order or in the interest of national security.

106 Chapter VII of the Act (Sections 34 to 47) provides for offences and penalties. Section 34 provides for penalty for impersonation at the time of enrolment. Section 35 provides a penalty for impersonation of an Aadhaar number holder by changing demographic or biometric information. Under Section 37, a penalty for disclosing identity information (which was collected in the course of enrolment or authentication) is provided. Section 38 provides a penalty for unauthorised access to the CIDR. Section 39 imposes a penalty for tampering with data in the CIDR. Under Sections 40 and 41, a penalty has been provided for requesting entities and enrolment agencies, in case they act in contravention of the obligations imposed upon them under the Act. Section 44 indicates that the provisions of the Act would apply to any offence or contravention committed outside India by any person, irrespective of nationality.

107 Section 48 empowers the Central Government to supersede UIDAI in certain situations. Section 50 states that UIDAI is bound by directions on questions of policy given by the Central Government. Section 51 authorizes the UIDAI to delegate to any member, officer of the Authority or any other person, such of its powers and functions (except the power under section 54) as it may deem necessary. Section 53 empowers the Central Government to make rules to carry out the provisions of the Act. Under Section 54(2)(m), UIDAI can make regulations providing the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits,

services and “other purposes” for which Aadhaar numbers may be used. Section 57 authorizes the State or any body corporate or person to use an Aadhaar number for establishing the identity of an individual “for any purpose”, subject to the procedure and obligations under Section 8 and Chapter VI of the Act. Section 59 seeks to validate the actions taken by the Central Government pursuant to the notifications dated 28 January 2009 and 12 September 2015, and prior to the enactment of the Aadhaar Act.

This broad description of the provisions of the Aadhaar Act indicates that the Act creates a framework for obtaining a unique identity number - the Aadhaar number - by submitting demographic and biometric information and undergoing the process of enrolment and authentication. The Act indicates that the Aadhaar number may be accepted as proof of identity for any purpose. The Act, in other words, creates a platform for one pan-India and nationally acceptable identity. It creates a central database (CIDR) for storage of identity information collected from individuals. Sections 3 to 6 specifically deal with the process of **enrolment**. Section 3 entitles every resident to hold an Aadhaar number. Section 4(3) states that the Aadhaar number so generated may be used as a proof of identity “for any purpose”. The primary object of the legislation is to create one national identity for every resident. It seeks to do so by legislating a process for collecting demographic and biometric information. The Act has created an authority to oversee the fulfilment of its provisions. In its primary focus and initiatives, the law traverses

beyond the territory reserved by Article 110 for a Money Bill. Sections 7 to 10 deal with **authentication** of information submitted at the time of enrolment. Section 8 creates **obligations on requesting entities** to ensure that **consent is obtained** from individuals before collecting their identity information and that the identity information of such individual is only used for submission to the CIDR for authentication. Sections 11 to 23 **create a statutory authority** (UIDAI) and assign responsibilities to it for the processes of enrolment and authentication and to discharge other functions assigned to it under the Act, including developing the policy, procedure and systems for issuing Aadhaar numbers to individuals. Section 23(2)(h) provides that apart from availing of various subsidies, benefits, and services, Aadhaar numbers may be used for "other purposes". Sections 28 to 33 deal with protection of information, and provide for security and confidentiality of identity information and restrictions on sharing of information. Section 28 imposes obligations on the UIDAI to ensure the **security** and **confidentiality** of identity information and authentication records of individuals, which are in its **possession** or **control**, including information **stored** in CIDR. **Disclosure** of identity information and authentication records can be made under Section 33, pursuant to a **court order** (not below the rank of District Judge) or in the **interest of national security** in pursuance of a direction of an officer (not below the rank of Joint Secretary to the Government of India). Sections 34 to 47 deal with substantive **offences and penalties** created under the Act. Sections 54(2)(m) states that regulations can be made by UIDAI specifying the manner of use of Aadhaar

numbers for the purposes of providing or availing of various subsidies, benefits, services and "other purposes" for which Aadhaar numbers may be used. Section 57 authorizes the use of Aadhaar number by anyone (whether by the State or any body corporate or person under law or contract) for establishing the identity of an individual "for any purpose".

108 Section 7 makes the use of the Aadhaar number mandatory for availing subsidies, benefits or services, for which expenditure is incurred from the Consolidated Fund of India. The scheme of the Act deals with several aspects relating to the unique identity number. The unique identity is capable of being used for **multiple purposes**: availing benefits, subsidies and services, for which expenses are incurred from the Consolidated Fund of India, is just one purpose, among others. The Preamble to the Aadhaar Act indicates that the main objective was to achieve an efficient and "targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India". The substantive provisions of the Act are, however, not confined to the object specified in the Preamble. Indeed, they travel far beyond the boundaries of a money bill under Article 110(1). The enrolment on the basis of demographic and biometric information, generation of Aadhaar number, obtaining consent of individuals before collecting their individual information, creation of a statutory authority to implement and supervise the process, protection of information collected during the process, disclosure of information in certain circumstances, creation of offences and

penalties for disclosure or loss of information, and the use of the Aadhaar number for any purpose lie outside the ambit of Article 110. These themes are also not incidental to any of the matters covered by sub-clauses (a) to (f) of Article 110(1). The provisions of Section 57 which allow the use of an Aadhaar number by bodies corporate or private parties for any purpose do not fall within the ambit of Article 110. The legal framework of the Aadhaar Act creates substantive obligations and liabilities which have the capability of impacting on the fundamental rights of residents.

109 A Bill, to be a Money Bill, must contain only provisions which fall within the ambit of the matters mentioned in Article 110. Section 7 of the Act allows the Aadhaar number to be made mandatory for availing of services, benefits and subsidies for which expenditure is incurred from the Consolidated Fund of India. Under clause (e) of Article 110(1) the money bill must deal with the declaring of any expenditure to be expenditure charged on the Consolidated Fund of India (or increasing the amount of expenditure). Significantly, Section 7 does not declare the expenditure incurred on services, benefits or subsidies to be a charge on the Consolidated Fund of India. What Section 7 does is to enact a provision allowing for Aadhaar to be made mandatory, in the case of services, benefits or subsidies which are charged to the Consolidated Fund. Section 7 does not declare them to be a charge on the Consolidated Fund. It provides that in the case of services, benefits or subsidies which are already charged to the Consolidated Fund, Aadhaar can be made mandatory to avail

of them. Section 7, in other words, is a provision for imposing a requirement of authentication and not declaring any expenditure to be a charge on the Consolidated Fund of India. Hence, even Section 7 is not within the ambit of Article 110(1)(e). However, even if Section 7 were to be held to be referable to Article 110, that does not apply to the other provisions of the Act. The other provisions of the Act do not in any event fall within the ambit of Article 110(1). Introducing one provision – Section 7 – does not render the entirety of the Act a Money Bill where its other provisions travel beyond the parameters set out in Article 110. Section 57 of the Act in particular (which creates a platform for the use of the Aadhaar number by the private entities) can by no stretch of logic be covered under Article 110(1). The other provisions of the Act do not deal with that which has been provided under Sub-clauses (a) to (g) of Article 110. As regards the 'incidental' provision under Article 110(1)(g), the provisions of the Aadhaar Act are not "incidental to any of the matters specified in sub-clauses (a) to (f)". Even if it is assumed that there is one provision (Section 7) which is relatable to sub-clause (e) of Article 110(1), the other provisions of the Act are unrelated to Article 110(1).

110 This Court must also advert to the legislative history prior to the enactment of the Aadhaar Act. An attempt to provide a legislative framework governing the Aadhaar project was first made by introducing the National Identification Authority of India Bill, 2010 ("NIA Bill"). The NIA Bill was

introduced in the Rajya Sabha on 3 December 2010. The Preamble of the Bill indicated its purpose:

> "A Bill to provide for the establishment of the National Identification Authority of India for the purpose of issuing identification numbers to individuals residing in India and to certain other classes of individuals and manner of authentication of such individuals to facilitate access to benefits and services to such individuals to which they are entitled and for matters connected therewith or incidental thereto."

The main objective of the Bill was to establish the National Identification Authority of India to issue unique identification numbers (called 'Aadhaar') to residents of India and to any other category of people for the purpose of facilitating access to benefits and services. Chapter II (Clauses 3 to 10) of the Bill dealt with Aadhaar numbers. Clause 3 of the Bill entitled every resident to obtain an Aadhaar number on providing demographic and biometric information to the Authority in such manner as may be specified. Clause 4(3) stated that an Aadhaar number shall be accepted, subject to authentication, as proof of identity of the Aadhaar number holder. Chapter III (Clauses 11 to 23) dealt with the National Identification Authority of India. Clause 11 provided for establishment of the Authority by the Central Government. Clause 23 empowered the Authority to develop the policy, procedure and systems for issuing Aadhaar numbers to residents and to perform authentication. Clause 23(2)(h) stated that the Authority may specify the usage and applicability of the Aadhaar number for delivery of various benefits and services. Establishing, operating and maintaining of the Central Identities Data Repository (CIDR) by the Authority was provided under Clause 23(2)(j).

Chapter IV (Clauses 24 to 27) provide for grants, accounts and audit and annual reports related to the Authority. Clause 25 stated that the fees or revenue collected by the Authority shall be credited to the Consolidated Fund of India and the entire amount would be transferred to the Authority. Chapter V (Clauses 28 and 29) dealt with creation of an Identity Review Committee and its functions. The functions of the Review Committee included ascertaining the extent and pattern of usage of Aadhaar numbers across the country and preparing a report annually along with recommendations. Chapter VI (Clauses 30 to 33) dealt with the protection of individual identity information and authentication records. Clause 30(1) required the Authority to ensure the security and confidentiality of identity information and authentication records of individuals. Clause 30(2) required the Authority to take measures (including security safeguards) to ensure that the information in the possession or control of the Authority (including information stored in the Central Identities Data Repository) is secured and protected against any loss or unauthorised access or use or unauthorised disclosure. Clause 33 stated that individual information may be disclosed pursuant a court order or in the interest of national security. Chapter VII (Clauses 34 to 46) created offences and penalties under the law. Clause 47 empowered the Central Government to supersede the Authority. Clause 50 authorized the Authority to delegate to any Member, officer of the Authority or any other person such of its powers and functions (except the power under Clause 53). Clause 57 sought to validate

actions taken by the Central Government under the Planning Commission's notification of 2009.

111 Since the UID programme involved complex issues, the NIA Bill was referred, on 10 December 2010, to the Standing Committee on Finance, chaired by Mr Yashwant Sinha, for examination and report. The Standing Committee comprised of 21 members from the Lok Sabha and 10 members from the Rajya Sabha. The Standing Committee submitted its Report[175] on 11 December 2011. The Report raised several objections to the Bill, which included those summarised below:

(i) Since law making was underway, the bill being pending, any executive action is as violative of Parliament's prerogatives as promulgation of an ordinance while one of the Houses of Parliament is in session;

(ii) While the country is facing a serious problem of illegal immigrants and infiltration from across the borders, the National Identification Authority of India Bill, 2010 proposes to entitle every resident to obtain an Aadhaar number, apart from entitling such other category of individuals as may be notified from time to time. This will, it is apprehended, make even illegal immigrants entitled for an Aadhaar number;

(iii) The issue of a unique identification number to individuals residing in India and other classes of individuals under the Unique Identification (UID)

[175] Forty-Second Report, Standing Committee on Finance (2011-12), available at http://www.prsindia.org/uploads/media/UID/uid%20report.pdf

Scheme is riddled with serious lacunae and concern areas. For example, the full or near full coverage of marginalized sections for issuing Aadhaar numbers could not be achieved mainly due to two reasons viz. (a) the UIDAI doesn't have the statistical data relating to them; and (b) estimated failure of biometrics is expected to be as high as 15% because a large chunk of population is dependent on manual labour;

(iv) Despite the presence of serious differences of opinion within the Government on the UID scheme, the scheme continues to be implemented in an overbearing manner without regard to legalities and other social consequences;

(v) The UID scheme lacks clarity on many issues including even the basic purpose of issuing an "Aadhaar" number. Although the scheme claims that obtaining an Aadhaar number is voluntary, an apprehension has developed in the minds of people that in future, services / benefits including food entitlements would be denied in case they do not an have an Aadhaar number;

(vi) It is also not clear as to whether possession of an Aadhaar number would be made mandatory in future for availing of benefits and services. Even if the Aadhaar number links entitlements to targeted beneficiaries, it may not ensure that beneficiaries have been correctly identified. Thus, the present problem of proper identification would persist;

(vii) Though there are significant differences between the identity system of other countries and the UID scheme, yet there are lessons from the global experience to be learnt before proceeding with the implementation of the UID scheme, which the Ministry of Planning has ignored completely;

(viii) Considering the huge database and possibility of misuse of information, the enactment of a national data protection law is a pre-requisite for any law that deals with large scale collection of information from individuals and its linkages across separate databases. In the absence of data protection legislation, it would be difficult to deal with issues like access to and misuse of personal information, surveillance, profiling, linking and matching of data bases and securing confidentiality of information;

(ix) The Standing Committee strongly disapproved of the hasty manner in which the UID scheme was approved. Unlike many other schemes / projects, no comprehensive feasibility study, which ought to have been done before approving such an expensive scheme, was done involving all aspects of the UID scheme including a cost-benefit analysis, comparative costs of Aadhaar numbers and various existing forms of identity, financial implications and prevention of identity theft, for example, using hologram enabled ration cards to eliminate fake and duplicate beneficiaries;

(x) The UID scheme may end up being dependent on private agencies, despite contractual agreements made by the UIDAI with several private

vendors. As a result, the beneficiaries may be forced to pay over and above the charges to be prescribed by the UIDAI for availing of benefits and services, which are now available free of cost;

(xi) The scheme is full of uncertainty in technology as a complex scheme is built up on untested and unreliable technology and on several assumptions. It is also not known as to whether the proof of concept studies and assessment studies undertaken by the UIDAI have explored the possibilities of maintaining accuracy to a large level of enrolment of 1.2 billion people; and

(xii) The Committee felt that entrusting the responsibility of verification of information of individuals to the registrars to ensure that only genuine residents get enrolled into the system may have far reaching consequences for national security. Given the limitation of any mechanism such as a security audit by an appropriate agency that would be set up for verifying the information, it is not evident as to whether a complete verification of information of all Aadhaar number holders is practically feasible; and whether it would deliver the intended results without compromising national security.

With these apprehensions about the UID scheme, the Standing Committee on Finance categorically conveyed that the National Identification Authority of India Bill, 2010 was not acceptable. The Committee urged the Government to

reconsider and review the UID scheme and the proposals contained in the Bill and bring forth a fresh legislation before Parliament. Ultimately, the NIA Bill was withdrawn from the Rajya Sabha on 3 March, 2016.

112 A comparison of the Aadhaar Act 2016 and NIA Bill 2010 reveals that both have a common objective and framework – establishing a system of unique identity numbers, which would be implemented and monitored by a statutory authority. The NIA Bill was not a Money Bill. It was never passed by the Rajya Sabha. The Bill was scrutinized by a Standing Committee on Finance, which had 10 members from the Rajya Sabha and 21 from the Lok Sabha. The NIA Bill did not contain a provision, similar to Section 7 of the Aadhaar Act. Yet, as discussed earlier, the presence of Section 7 does not make the Aadhaar Act a Money Bill. Introducing the Aadhaar Act as a Money Bill deprived the Rajya Sabha of its power to reject or amend the Bill. Since the Aadhaar Act in its current form was introduced as a Money Bill in the Lok Sabha, the Rajya Sabha had no option other than of making recommendations to the Bill. The recommendations made by the Rajya Sabha (which also included deletion of Section 57) were rejected by the Lok Sabha. The legislative history is a clear pointer to the fact that the subsequent passage of the Bill as a Money Bill by-passed the constitutional authority of the Rajya Sabha. The Rajya Sabha was deprived of its legitimate constitutional role by the passage of the Bill as a Money Bill in the Lok Sabha.

113 The Court must also address the contention of the Respondents that the Aadhaar Act is “in pith and substance” a Money Bill. The learned Attorney General for India has submitted that though the Act has ancillary provisions, its main objective is the delivery of subsidies, benefits and services flowing out of the Consolidated Fund of India and that the other provisions are related to the main purpose of the Act which was giving subsidies and benefits. It has been submitted that the real test to be applied in the present dispute is the doctrine of pith and substance.

114 This Court has applied the doctrine of pith and substance when the legislative competence of a legislature to enact a law is challenged. The doctrine is applied to evaluate whether an enactment which is challenged falls within an entry in one of the three Lists in the Seventh Schedule over which the legislature has competence under Article 246 of the Constitution. The Seventh Schedule to the Constitution distributes legislative powers between the Union and the States. When a law enacted by a legislature is challenged on the ground of a lack of legislative competence, the doctrine of pith and substance is invoked. Under the doctrine, the law will be valid if in substance, it falls within the ambit of a legislative entry on which the legislature is competent to enact a law, even if it incidentally trenches on a legislative entry in a separate list. The constitutional rationale for the application of this

doctrine has been explained in a Constitution Bench decision of this Court in **A S Krishna** v **State of Madras**[176]:

> "8…But then, it must be remembered that we are construing a federal Constitution. **It is of the essence of such a Constitution that there should be a distribution of the legislative powers of the Federation between the Centre and the Provinces.** The scheme of distribution has varied with different Constitutions, but even when the Constitution enumerates elaborately the topics on which the Centre and the States could legislate, some overlapping of the fields of legislation is inevitable. The British North America Act, 1867, which established a federal Constitution for Canada, enumerated in Sections 91 and 92 the topics on which the Dominion and the Provinces could respectively legislate. **Notwithstanding that the lists were framed so as to be fairly full and comprehensive, it was not long before it was found that the topics enumerated in the two sections overlapped, and the Privy Council had time and again to pass on the constitutionality of laws made by the Dominion and Provincial legislatures. It was in this situation that the Privy Council evolved the doctrine, that for deciding whether an impugned legislation was intra vires, regard must be had to its pith and substance. That is to say, if a statute is found in substance to relate to a topic within the competence of the legislature, it should be held to be intra vires, even though it might incidentally trench on topics not within its legislative competence...**" (Emphasis supplied)

The decision of a three judge Bench of this Court in **State of Maharashtra** v **Bharat Shanti Lal Shah**[177] has summarized the process of reasoning which must be followed by the Court while applying the doctrine of pith and substance. The Court held:

> "43…If there is a challenge to the legislative competence the courts will try to ascertain the pith and substance of such enactment on a scrutiny of the Act in question. **In this process, it is necessary for the courts to go into and examine the true character of the enactment, its object, its scope and effect to find out whether the enactment in**

[176] 1957 SCR 399
[177](2008) 13 SCC 5

> **question is genuinely referable to the field of legislation allotted to the respective Legislature under the constitutional scheme.** Where a challenge is made to the constitutional validity of a particular State Act with reference to a subject mentioned in any entry in List I, the court has to look to the substance of the State Act and on such analysis and examination, if it is found that in the pith and substance, it falls under an entry in the State List but there is only an incidental encroachment on topics in the Union List, the State Act would not become invalid merely because there is incidental encroachment on any of the topics in the Union List."[178] (Emphasis supplied)

115 The doctrine of pith and substance is mainly used to examine whether the legislature has the competence to enact a law with regard to any of the three Lists provided under the Constitution. It cannot be applied to sustain as a Money Bill, a Bill which travels beyond the constitutional boundaries set out by Article 110 Whether a Bill is validly passed as a Money Bill has nothing to do with the legislative competence of the legislature under Article 246 of the Constitution. Whether a Bill is a Money Bill has to be tested within the boundaries of Article 110. The submission of the Attorney General boils down to this: 'ignore the expression "only provisions dealing with all or any of the following matters" and hold the Bill to be a Money Bill by treating Section 7 as its dominant provision'. This cannot be accepted. This would ignore the express and clear language of Article 110. As we have emphasised earlier, the submission of the Attorney General requires the court to transpose the word "only" from its present position to a place before "if". That would be to rewrite the Constitution to mean that a Bill would be a Money Bill if it contained some provisions which fall under sub-clauses (a) to (g). The

[178] Ibid, at page 21

Constitution says to the contrary: a Bill is a Money Bill if it contains "only provisions" dealing with one or more of the matters set out in sub-clauses (a) to (g). Looked at in another way, all the provisions of the Aadhaar Act (apart from Section 7) cannot be read as incidental to Section 7. Such a view is belied by a plain reading of the Act, as indicated earlier. Moreover, we have also indicated reasons why even Section 7 cannot be held to be referable to Article 110. Section 7 does not deal with the declaring of any expenditure as expenditure charged to the Consolidated Fund. Section 7 allows for making Aadhaar mandatory for availing of subsidies, benefits or services the expenditure incurred on which is charged to the Consolidate Fund. Section 7 does not charge any expenditure to the Consolidated Fund. It deals with making Aadhaar mandatory.

In support of their contention, the Respondents have also relied upon a two judge Bench decision in **Union of India** v **Shah Goverdhan L Kabra Teachers' College**[179] to submit that the doctrine of pith and substance can be used in any context. The Court held:

> "7. It is further a well-settled principle that entries in the different lists should be read together without giving a narrow meaning to any of them. Power of the Parliament as well as the State legislature are expressed in precise and definite terms. While an entry is to be given its widest meaning but it cannot be so interpreted as to over-ride another entry or make another entry meaningless and in case of an apparent conflict between different entries, it is the duty of the court to reconcile them. When it appears to the Court that there is apparent overlapping between the two entries the doctrine of "pith and substance" has to be applied to find out the true nature of a legislation and the entry with which it would fall. In

[179] (2002) 8 SCC 228

> case of conflict between entries in List I and List II, the same has to be decided by application of the principle of "pith and substance". **The doctrine of "pith and substance" means that if an enactment substantially falls within the powers expressly conferred by the Constitution upon the legislature which enacted it, it cannot be held to be invalid, merely because it incidentally encroaches on matters assigned to another legislature.** When a law is impugned as being ultra-vires of the legislative competence, what is required to be ascertained is the true character of the legislation. If on such an examination it is found that the legislation is in substance one on a matter assigned to the legislature then it must be held to be valid in its entirety even though it might incidentally trench on matters which are beyond its competence. In order to examine the true character of the enactment, the entire Act, its object and scope and effect, is required to be gone into. The question of invasion into the territory of another legislation is to be determined not by degree but by substance. **The doctrine of "pith and substance' has to be applied not only in cases of conflict between the powers of two legislatures but in any case where the question arises whether a legislation is covered by particular legislative power in exercise of which it is purported to be made.**"[180] (Emphasis supplied)

The decision is of no assistance to the submission in the present dispute. The observations made by the Court are in relation to the power to legislate under Article 246 of the Constitution. It is unconnected to the question of a Money Bill. Therefore, the argument that the Aadhaar Act is "in pith and substance" a Money Bill is rejected.

116 Introducing the Aadhaar Act as a Money Bill has bypassed the constitutional authority of the Rajya Sabha. The passage of the Aadhaar Act as a Money Bill is an abuse of the constitutional process. It deprived the Rajya Sabha from altering the provisions of the Bill by carrying out amendments. On the touchstone of the provisions of Article 110, the Bill could not have been

[180] Ibid, at pages 233-234

certified as a Money Bill. In his last address to the Constituent Assembly on 25 November 1949, Dr B R Ambedkar had stated:

> "The working of a Constitution does not depend wholly upon the nature of the Constitution. The Constitution can provide only the organs of State such as the Legislature, the Executive and the Judiciary. The factors on which the working of those organs of the State depends are the people and the political parties they will set up as their instruments to carry out their wishes and their politics."[181]

117 The Rajya Sabha has an important role in the making of laws. Superseding the authority of the Rajya Sabha is in conflict with the constitutional scheme and the legitimacy of democratic institutions. It constitutes a fraud on the Constitution. Passing of a Bill as a Money Bill, when it does not qualify for it, damages the delicate balance of bicameralism which is a part of the basic structure of the Constitution. The ruling party in power may not command a majority in the Rajya Sabha. But the legislative role of that legislative body cannot be obviated by legislating a Bill which is not a Money Bill as a Money Bill. That would constitute a subterfuge, something which a constitutional court cannot countenance. Differences in a democratic polity have to be resolved by dialogue and accommodation. Differences with another constitutional institution cannot be resolved by the simple expedient of ignoring it. It may be politically expedient to do so. But it is constitutionally impermissible. This debasement of a democratic institution cannot be allowed to pass. Institutions are crucial to democracy. Debasing them can only cause a peril to democratic structures.

[181] Constituent Assembly (25 November 1949)

The Act thus fails to qualify as a Money Bill under Article 110 of the Constitution. Since the Act was passed as a Money Bill, even though it does not qualify to be so, the passage of the Act is an illegality. The Aadhaar Act is in violation of Article 110 and therefore is liable to be declared unconstitutional.

F Biometrics, Privacy and Aadhaar

> "Any situation that allows an interaction between man and machine is capable of incorporating biometrics"[182]

118 The term 'biometric' is derived from the Greek nouns 'βίος' (life) and 'μέτρον' (measure) and means 'measurement of living species'.[183] Biometric technologies imply that "unique or distinctive human characteristics of a person are collected, measured and stored for the automated verification of a claim made by that person for the identification of that person."[184] These systems thus identify or verify the identity or a claim of persons on the basis of the automated measurement and analysis of their biological traits (such as fingerprints, face and iris) or behavioral characteristics (such as signature and voice).

[182] Gary Roethenbaugh, (cited in A. Cavoukian, Privacy and Biometrics, Information and Privacy Commissioner, Ontario, Canada, 1999, page 11, available at http://www.ipc.on.ca/images/Resources/pri- biom.pdf
[183] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, Springer (2013)
[184] Ibid.

119 The idea that parts of our body can be used to identify our unique selves is not new. Prints of hand, foot and finger have been used since ancient times because of their unique characteristics. Before the advent of biometric systems, however, human characteristics were compared in a manual way. Today's biometric systems hence differ from manual verification methods in that technology allows for automated comparison of human characteristic(s) in place of a regime of manual verification that existed earlier. It must be understood that biometric systems themselves do not identify individuals. For identification, additional information which is already stored in databases is needed since biometric systems can only compare information which is already submitted.[185] Integral to such a system is the matching of a claim of identity with biometric data collected and stored earlier.

In general, biometric applications are referred to as systems which allow one to authenticate claims. The verb 'to authenticate' can be described as 'making authentic, legally valid'.[186] Originally, fingerprints were the most commonly known and used biometric traits, but with improvements in technology, multiple sources of biometric information have emerged. These include data related to facial features, iris, voice, hand geometry and DNA. Each trait is collected using different technologies and can be used for different purposes

[185] Ibid.
[186] Ibid.

separately or in combination, to strengthen and improve the accuracy and reliability of the identification process.[187]

In general, biometric information is developed by processing extractable key features of an individual into an ‘electronic digital template’, which is then encrypted and stored in a database. When an individual connects with the system to verify his/her identity for any purpose, the information is used by matching the ‘electronic digital template’ saved with the biometric information presented, based on which comparison, the individual’s identity will be confirmed or rejected. The intended purpose of biometric technology is to confirm the identity of individuals through a “one to one” identification check. This system compares a source of biometric data with existing data for that specific person.

F.I Increased use of biometric technology

120 There had been an initial increase in the usage of biometric technology in both developed and developing countries by both the private and the public sector. However, despite the increased adoption of biometric technologies by developed countries in the 1980s and 1990s, recent trends depict their reluctance to deploy biometric technology - or at least mass storage of biometric data - because of privacy concerns.[188] Key instances included the

[187] Nancy Yue Liu, Bio-Privacy: Privacy Regulations and the Challenge of Biometrics, Routledge (2013).
[188] Privacy International, Biometrics: Friend or foe of privacy?, available at https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf

scrapping of the National Identity Register and ID cards in the UK, and Germany's decision to reject a centralised database when deploying biometric passports.[189] By contrast, in developing countries there is a rise in the deployment of biometric technology since it is being portrayed to citizens as a means to establishing their legal identity and providing them access to services, as well as a tool for achieving economic development. However, too often these goals are prioritised at the expense of their right to privacy and other human rights.[190] Simon Davies, an eminent privacy expert, points out that it is not an accident or coincidence that biometric systems are most aggressively tried out with welfare recipients since they are not in a position to resist the State-mandated intrusion.[191]

There has been a particular increase in the use of biometric technology in identification programs in developing countries. This is because "biometrics include a wide range of biological measures which are considered sufficiently unique at a population level to allow individual identification with high rates of accuracy".[192] Lack of formal identification and official identity documentation in the developing world is a serious challenge which impedes the ability of governments as well as development organisations to provide essential goods and services to the populations they serve.[193] Further, identification is also

[189] Ibid
[190] Ibid
[191] Simon Davies, as cited in John D. Woodward, Biometric Scanning, Law & Policy: Identifying the Concerns - Drafting the Biometric Blueprint, University of Pittsburgh Law Review, (1997)
[192] Daniel M. L Storisteanu, Toby L. Norman, Alexandra Grigore and Alain B. Labrique, Can biometrics beat the developing world's challenges?, Biometric Technology Today (2016)
[193] Ibid

essential to the gathering of accurate data which is required for monitoring the progress of government programmes.[194] However, while biometric technology brings many advantages, the flip side is that the same technology can also lead to human rights violations:

> "When adopted in the absence of strong legal frameworks and strict safeguards, biometric technologies pose grave threats to privacy and personal security, as their application can be broadened to facilitate discrimination, profiling and mass surveillance. The varying accuracy and failure rates of the technology can lead to misidentification, fraud and civic exclusion."[195]

121 The adoption of biometric technologies in developing countries in particular poses unique challenges since the implementation of new technologies in these countries is rarely preceded by the enactment of robust legal frameworks. Assessments of countries where a legal mechanism to regulate new technologies or protect data has followed as an afterthought have shown that there exists a huge risk of mass human rights violations where individuals are denied basic fundamental rights, and in extreme cases, even their identity.[196]

122 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

[194] Ibid
[195] Privacy International, Biometrics, available at https://privacyinternational.org/topics/biometrics
[196] Privacy International, Biometrics: Friend or foe of privacy?, available at https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf

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.[197]

123 Privacy has been recognized as a fundamental human right in various national constitutions and numerous global and regional human rights treaties. In today's digital age, the right to privacy is "the cornerstone that safeguards who we are and supports our on-going struggle to maintain our autonomy and self-determination in the face of increasing state power."[198]

124 The proliferation of biometric technology has facilitated the invasion of individual privacy at an unprecedented scale. The raw information at the heart of biometrics is personal by its very nature.[199] The Aadhaar Act recognises this as sensitive personal information. Biometric technology is unique in the sense that it uses part of the human body or behaviour as the basis of authentication or identification and is therefore intimately connected to the

[197] Ibid
[198] Privacy International, Biometrics: Friend or foe of privacy?, available at https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf
[199] Nancy Yue Liu, Bio-Privacy: Privacy Regulations and the Challenge of Biometrics, Routledge (2013)

individual concerned. While biometric technology raises some of the same issues that arise when government agencies or private firms collect any personal information about citizens, there are specific features that distinguish biometric data from other personal data, making concerns about biometric technology of particular importance with regard to privacy protection.[200]

125 There are two main groups of privacy- related interests that are directly pertinent to the contemporary discussion on the ethical and legal implications of biometrics.[201] The first group falls under 'informational privacy' and is concerned with control of personal information. The ability to control personal information about oneself is closely related to the dignity of the individual, self-respect and sense of personhood. The second interest group falls under the rubric of 'physical privacy'. This sense of privacy transcends the purely physical and is aimed essentially at protecting the dignity of the human person. It is a safeguard against intrusions into persons' physical bodies and spaces. Another issue is of property rights with respect to privacy, which concerns the appropriation and ownership of interests in human personality. In many jurisdictions, the basis of informational privacy is the notion that all information about an individual is in some fundamental way their own property, and it is theirs to communicate or retain as they deem fit.

[200] Ibid
[201] Ibid

126 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.

127 Concerns about physical privacy usually take a backseat as compared to concerns about informational privacy. The reason for this is that physical intrusion resulting from the use of biometric technology usually results from the collection of physical information. However, for some people of specific

cultural or religious backgrounds, even the mental harm resulting from physical intrusion maybe quite serious.[202]

Another concern is that the widespread usage of biometrics substantially undermines the right to remain anonymous.[203] People desire anonymity for a variety of reasons, including that it is fundamental to their sense of freedom and autonomy. Anonymity may turn out to be the only tool available for ordinary people to defend themselves against being profiled. Thus, it is often argued that biometric technology should not be the appropriate choice of technology as biometrics by its very nature is inconsistent with anonymity. Given the manner in which personal information can be linked and identified using biometric data, the ability to remain anonymous is severely diminished. While some argue that "it is not obvious that more anonymity will be lost when biometrics are used", this argument may have to be evaluated in light of the fact that there is no existing identifier that can be readily equated with biometrics.[204] No existing identifier can expose as much information as biometric data nor is there any other identifier that is supposed to be so universal, long-lasting and intimately linked as biometrics. To say that the use of biometrics will not cause further loss of anonymity may thus be overly optimistic. Semi-anonymity maybe possible, provided that the biometric system is carefully designed from the inception.

[202] Nancy Yue Liu, Bio-Privacy: Privacy Regulations and the Challenge of Biometrics, Routledge (2013).
[203] Ibid
[204] Ibid

Another significant change brought about by biometric technology is the precipitous decline of 'privacy by obscurity', which is essentially "a form of privacy afforded to individuals inadvertently by the inefficiencies of paper and other legacy recordkeeping." [205] Now that paper records worldwide are giving way to more efficient digital record-keeping and identification, this form of privacy is being extinguished, and sometimes without commensurate data privacy protections put in place to remedy the effects of the changes."[206]

128 Biometrically enhanced identity information, combined with demographic data such as address, age and gender, among other data, when used in increasingly large, automated systems creates profound changes in societies, particularly in regard to data protection, privacy, and security. Biometrics are at the very heart of identification systems. There are numerous instances in history where the persecution of groups of civilians on the basis of race, ethnicity and religion was facilitated through the use of identification systems. There is hence an alarming need to ensure that the on-going development of identification systems be carefully monitored, while taking into account lessons learnt from history.

129 It is important to justify the usage of biometric technology given the invasion of privacy. When the purpose of collecting the biometric data is just for authentication and there is little or no benefit in having stronger user

[205] Pam Dixon, A Failure to Do No Harm – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S., Health and Technology (2017), Vol. 7, at pages 539–567

[206] Ibid.

identification, it is difficult to justify the collection of biometric information. The potential fear is that there are situations where there are few or no benefits to be gained from strong user verification / identification and this is where biometric technology may be unnecessary.[207] (Example: When ascertaining whether an individual is old enough to go to a bar and drink alcohol, it is unnecessary to know who the person is, when all that is needed to be demonstrated is that the individual is of legal age). Fundamental rights are likely to be violated in case biometrics are used for applications merely requiring a low level of security.

130 Biometric data, by its very nature, is intrinsically linked to characteristics that make us 'humans' and its broad scope brings together a variety of personal elements. It is argued that the collection, analysis and storage of such innate data is dehumanising as it reduces the individual to but a number. Ultimately, organisations and governmental agencies must demonstrate that there is a compelling legitimate interest in using biometric technology and that an obligatory fingerprint requirement is reasonably related to the objective for which it is required. One way of avoiding unnecessary collection of biometric data is to set strict legal standards to ensure that the intrusion into privacy is commensurate with and proportional to the need for the collection of biometric data.[208]

[207] Nancy Yue Liu, Bio-Privacy: Privacy Regulations and the Challenge of Biometrics, Routledge (2013).
[208] Ibid

F.2 Consent in the collection of biometric data

131 Rules on the collection of physical data by government agencies usually specify under what conditions a person can be required to provide fingerprints and/or bodily tissues**.** If consent is required, rules are in place to regulate the scope of consent. If forced searches are allowed, specifications are usually provided as to how and by whom the search will be performed. Therefore, the legal questions surrounding the issue should be:

(a) If required, what exactly should be the extent of coverage of the consent?

(b) When is the compulsory collection of biometric information required and who is eligible to conduct it?

(c) What is the procedure to do so?

(d)What exactly should be filed and stored?

132 Biometric technology is far from being a mature technology and a variety of errors inevitably occur. Mature technology is a popular term for any technology for which any improvements in deployment are evolutionary rather than revolutionary.[209] Once a biometric system is compromised, it is compromised forever. In the event of biometric identity theft, there would appear to be no alternative but to withdraw the user from the system**.** Passwords and numbers can be changed, but how does one change the basic biological features that compromise biometrics in the event that there is a theft?

[209] Segen's Medical Dictionary, 2012.

All of these parameters need to be applied to test the validity of the Aadhaar legislation in a two-part inquiry: First, reports and steps taken by the Government of India that guided the introduction and role of biometrics before the enactment of the Aadhaar Act will be analysed, which will be followed by an analysis of relevant provisions concerning the intersection of biometric technology and privacy, as they are enshrined in the Aadhaar Act, 2016 and supporting Regulations made under it.

F.3 Position before the Aadhaar legislation

Summary of Pre-Enactment Events

133 On 3 March 2006, the Department of Information Technology, Ministry of Communications & Information Technology, gave its approval for implementation of the project 'Unique ID for Below Poverty Line Families' (BPL) by the National Informatics Centre over a period of 12 months.[210] This was followed by a Processes Committee being set up a few months later on 3 July 2006, to suggest the processes for updation, modification, addition and deletion of data from the core database to be created under the Unique ID ("**UID**") for BPL Families Project.[211] The Processes Committee prepared a

[210] Ministry of Communication & Information Technology, Department of Information Technology, Administrative Approval for the project - "Unique ID for BPL families", dated March 03, 2006 (Annexure R-1, List of Pre-enactment dates and events for the Aadhaar project submitted by the Learned AG).

[211] Department of Information Technology, Notification: Setting up of a Process Committee to suggest the processes for updation, modification, addition & deletion of data and fields from the core database to be created under the Unique ID for BPL families project, dated July 03, 2006 (Annexure R-2, List of Pre-enactment dates and events for the Aadhaar project submitted by the learned AG).

paper titled 'Strategic Vision: Unique Identification of Residents'[212]. The paper recommended the linkage of the UID database with other databases which would ensure continuous updation and user-based validation and use of the Election Commission's database as the base database.[213] The document inter-alia, also stated that statutory backing would be required for adoption of UID in the long term;[214] focus and conviction would be required on security and privacy to ensure adoption by different stakeholders;[215] while 'transparency vs. right to privacy' was another challenge that would have to be addressed.[216] Biometrics, however, found no mention in the paper at this stage.

Thereafter, on 4 December 2006, an Empowered Group of Ministers ("**EGoM**"), was constituted with the approval of the Prime Minister to collate the National Population Register ("**NPR**") under the Citizenship Act 1955 and the Unique Identification Number Project.[217] In its meeting held on 27 April 2007, the Processes Committee decided that the UID database would evolve in three stages: initial, intermediate and final. Biometrics was mentioned for the first time in the context of UID, when the committee agreed that if the infrastructure was available and the photograph and/or biometrics of a

[212] Strategic Vision: Unique Identification of Residents, dated 26 November 2006 (Annexure R-3, List of Pre-enactment dates and events for the Aadhaar project submitted by the learned AG).
[213] Ibid
[214] Ibid
[215] Ibid
[216] Ibid
[217] Constitution of an Empowered Group of Ministers to collate two schemes - the National Population Register under the Citizenship Act, 1955 and the Unique Identification Number (UID) project of the Department of Information Technology (Annexure R-4, List of Pre-enactment dates and events for the Aadhaar project submitted by the learned AG).

resident was obtainable along with other information, it would be captured in the initial and intermediate stages as well.[218] Subsequently, the EGoM approved the establishment of a UID Authority under the Planning Commission on 28 January 2008.[219] while the strategy to collate NPR and UID was also approved. The EGoM also agreed that the collection of data under the NPR exercise could include collection of photographs and biometrics to the extent feasible, while it was also resolved that the data collected under the NPR would be handed over to the UID Authority for maintenance and updation. The EGoM, in its fourth meeting dated 4 November 2008 decided that initially, the UIDAI will be established as an executive body under the Planning Commission for a period of 5 years. UIDAI, it was envisaged, will create its database from the electoral roll of the ECI and verify it through Below Poverty Line and Public Distribution System data, but it would also have the authority to take its own decisions as to how a database should be built.[220] Consequently, the Government of India issued a notification on 28 January 2009 constituting the UIDAI as an attached office and executive authority under the aegis of the Planning Commission.

[218] Planning Commission, No. 4(4)/56/2005- C&I, Minutes of the Fifth Meeting of the Unique ID project under the Chairmanship of Dr. Arvind Virmani (Annexure R-6, List of Pre-enactment dates and events for the Aadhaar project submitted by the learned AG).

[219] Minutes of the Second Meeting of the EGoM to collate two schemes - The National Population Register under the Citizenship Act, 1955 and the Unique Identification number (UID) project of the Department of Information Technology (Annexure R-10, List of Pre-enactment dates and events for the Aadhaar project submitted by the learned AG).

[220] Minutes of the Fourth Meeting of the EGoM to collate two schemes - The National Population Register under the Citizenship Act, 1955 and the Unique Identification Number (UID) project of the Department of Information Technology (Annexure R-12, List of Pre-enactment dates and events for the Aadhaar project submitted by the learned AG).

134 Following the constitution of UIDAI, the Secretary, Planning Commission addressed a letter to Chief Secretaries of all States/ UTs on 6 May 2009 enclosing a brief write up on UIDAI and UID numbers for resident Indians. The letter included the concept, implementation strategy, model of the project along with the role and responsibilities of the states/ UTs.[221] It was also decided that partner databases for two-way linkages between the UID database and the partner databases for maintenance and continuous updation of the UID databases would be ECI database, Ministry of Rural Development-rural household survey database and the State ration card (PDS) databases.

135 The first meeting of the PM's Council of UIDAI, was held on 12 August 2009. Various proposals were approved by the Council,[222] by which it was decided, among other things, that the proposal to designate UIDAI as an apex body to set standards in the area of biometrics and demographic data structures be approved. On 29 September 2009, UIDAI set up the Biometrics Standards Committee ("**BSC**") to frame biometric standards for UIDAI. The Committee was assigned with the following mandate:[223]

- To develop biometric standards that will ensure interoperability of devices, systems and processes used by various agencies that use the UID system.

[221] Secretary, Government of India, Planning Commission, D.O. No. A-11016/02/09-UIDAI (Annexure R-22, List of Pre-enactment dates and events for the Aadhaar project submitted by the learned AG).
[222] Planning Commission, Minutes of the meeting of the PM's Council of UIDAI (Annexure R-35, List of Pre-enactment dates and events for the Aadhaar project submitted by the Learned AG).
[223] Planning Commission, UIDAI, Office Memorandum, available at https://www.uidai.gov.in/images/resource/Biometric_Standards_Committee_Notification.pdf.

- To review the existing standards of Biometrics and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.

This was followed by the creation of the Demographic Data Standards and Verification Procedure Committee ("**DDSVPC**") on 9 October 2009, with the following mandate:[224]

- Review/ modify/ extend/ enhance the existing standards of Demographic data and recommend the Demographic Data standards (The data fields and their formats/structure, etc.) that will ensure interoperability and standardization of basic demographic data and their structure used by various agencies that use the UID system; and
- Recommend the Process of Verification of this demographic data in order to ensure that the data captured, at the time of enrolment of the residents into the UID system, is correct.

136 The DDSVPC in its report dated 9 December 2009, stated that UIDAI had selected biometrics features as the primary method to check for duplicate identity. In order to ensure that an individual was uniquely identified in an easy and cost-effective manner, it was necessary to ensure that the captured biometric information was capable of carrying out de-duplication at the time when information was collected.[225] The Know Your Resident ("**KYR**")

[224] DDSVPC (UIDAI), DDSVPC Report, dated 09 December 2009, available at https://uidai.gov.in/images/UID_DDSVP_Committee_Report_v1.0.pdf ,at pages 5-6.
[225] Ibid, at page 4

verification procedure was introduced to ensure that "*key demographic data is verified properly so that the data within UID system can be used for authentication of identity by various systems*". Three distinct methods of verification were to be acceptable under UID. Verification could be based on

- Supporting documents;
- An introducer system under which a network of "approved" introducers can introduce a resident and vouch for the validity of the resident's information; and (This idea was borrowed from the account opening procedure in the banks.)
- The process adopted for public scrutiny in the National Population Register.

137 In order to verify the correctness of certain mandatory fields, such as name, date-of-birth, and address, a "Proof of Identity" (PoI) and "Proof of Address" (PoA) would be required. This would comprise of documents containing the resident's name and photograph and the name and address, respectively. On 9 April 2010, the collection of iris biometrics for the NPR exercise was approved.[226]

138 A strategy overview issued by UIDAI in **April 2010** described the features, benefits, revenue model and timelines of the project.[227] The survey

[226] Annexure R-43, Volume II, List of Pre-enactment dates and events for the Aadhaar project, Submissions by the AG
[227] UIDAI, UIDAI Strategy Overview, available at http://www.prsindia.org/uploads/media/UID/UIDAI%20STRATEGY%20OVERVIEW.pdf.

outlined that UIDAI would collect the following demographic and biometric information from residents in order to issue a UID number:

- Name
- Date of birth
- Gender
- Father's/ Husband's/ Guardian's name and UID number (optional for adult residents)
- Mother's/ Wife's/ Guardian's name and UID number (optional for adult residents)
- Introducer's name and UID number (in case of lack of documents)
- Address
- **All ten fingerprints, photograph and both iris scans**

On 12 May 2010, a note outlining the background of UIDAI, and proposing an approach for collection of demographic and biometric attributes of residents for the UID project was submitted to the Cabinet Committee on UIDAI.[228] Permission of the Union Cabinet was sought to ensure that the approach which was proposed should be adhered to by the Registrar General of India for the NPR exercise and by all other Registrars in the UID system. The rationale behind the inclusion of iris biometrics and the need for capturing iris scans at the time of capturing biometric details was also explained.

This was followed by the introduction of the National Identification Authority of India Bill, 2010 (NIAI Bill) in the Rajya Sabha on 3 December 2010. On 13 February 2011, the one millionth Aadhaar card was delivered. Thereafter, on

[228] Annexure R-46, Volume II, List of Pre-enactment dates and events for the Aadhaar project, Submissions by the AG

11 April 2011, the Central Government notified the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ["**IT Rules**"] under Section 43A of the IT Act, 2000. On 29 September 2011, the Aadhaar project completed one year. An announcement was made of the generation of ten crore enrolments and of more than 3.75 crore Aadhaar numbers.

Analysis of UIDAI Reports & Rights of Registrars

A. Biometrics Standards Committee (BSC) Report

139 BSC in its report dated 30 December 2009 stated that it held extensive meetings and discussions with international experts and technology suppliers. A technical sub-group was formed to collect Indian fingerprints and analyze quality. Over 2,50,000 fingerprint images from 25,000 persons were sourced from the districts of Delhi, UP, Bihar and Orissa. Nearly all the images were from rural regions, and were collected by different agencies using different capture devices, and through different operational processes. The BSC report is silent about the pretext on which fingerprints of 25,000 people were collected. This action of UIDAI raises privacy concerns especially since the fingerprints were collected from rural regions where people may not have been aware or made aware by UIDAI before collection of fingerprints, of the possible privacy harms of giving up biometrics.

BSC after reviewing international standards and current national recommendations, concluded that a fingerprints-based biometric system was to be at the core of UIDAI's de-duplication efforts and that the ISO 19794 series of biometrics standards for fingerprints, face and iris set by the International Standards Organization (ISO) were most suitable for the UID project.[229] BSC also observed that while a fingerprints-based biometric system shall be at the core of UIDAI's de-duplication efforts, its accuracy in the Indian context could not predicted in the absence of empirical data:

> "The Committee notes that face is the most commonly captured biometric, and frequently used in manual checking. However, stand-alone, automatic face recognition does not provide a high level of accuracy, and can only be used to supplement a primary biometric modality. Fingerprinting, the oldest biometric technology, has the largest market share of all biometrics modalities globally. … Based on these factors, the Committee recognizes that a fingerprints-based biometrics system shall be at the core of the UIDAI's de-duplication efforts…
>
> The Committee, however, is also conscious of the fact that de-duplication of the magnitude required by the UIDAI has never been implemented in the world. In the global context, a de-duplication accuracy of 99% has been achieved so far, using good quality fingerprints against a database of up to fifty million. Two factors, however, raise uncertainty about the accuracy that can be achieved through fingerprints. First, retaining efficacy while scaling the database size from fifty million to a billion has not been adequately analyzed. Second, fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in depth in the Indian context."[230]

140 In its report for discussion titled "Technical Standards for Digital Identity Systems for Digital Identity", the Identification for Development (ID4D) initiative, a cross-departmental effort report of the World Bank, noted that

[229] UIDAI Committee on Biometrics, Biometrics Design Standards For UID Applications, at page 4
[230] Ibid.

UIDAI had not implemented "an important security standard, ISO 24745, which provides guidance for the protection of biometric information for confidentiality and integrity during storage or managing identities … due to the complexity of applicable compliance procedures" for the Aadhaar system.[231] Proponents of the program argue that in all fairness to UIDAI, it has to be noticed that the ISO 24745 standard was published in August 2011 whereas the report of BSC had already been submitted to UIDAI in January 2010. However, Mr. Myung Geun Chun, the Project Editor of ISO 24745, is reported to have stated that ISO 24745 standard is an 'invaluable tool' for addressing 'unique privacy concerns' like 'unlawful processing and use of data' raised by biometric identification because of its binding nature 'which links biometrics with personally identifiable information'.[232]

ISO 24745 seeks to "*safeguard the security of a biometric system and the privacy of data subjects with solid countermeasures*".[233] ISO 24745 standard specifies:

> - "Analysis of threats and countermeasures inherent in biometric and biometric system application models;
> - Security requirements for binding between a biometric reference and an identity reference;
> - Biometric system application models with different scenarios for the storage and comparison of biometric references;
> - Guidance on the protection of an individual's privacy during the processing of biometric information."[234]

[231] Identification for Development (World Bank Group), Technical Standards for Digital Identity Systems for Digital Identity Draft for Discussion, available at http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf, at page 22.
[232] Katie Bird, Is your biometric data safe online? ISO/IEC standard ensures security and privacy, (11 August 2011), available at https://www.iso.org/news/2011/08/Ref1452.html.
[233] Ibid.
[234] Ibid.

B. Strategy Overview of 2010

In this report, a balance was sought to be struck between ‘privacy and purpose’ in respect of the information of the residents which was collected. The report states that ‘agencies’ may store the information of the residents at the time of enrolment, but they will not have access to the information stored in the UID database.[235] Further, for the purposes of authentication, requests made by the agencies would be answered through a ‘Yes’ or a ‘No’ response only.[236] Under the sub-heading “Protecting Privacy and Confidentiality”, the report stated that the additional information which was being sought from people was only biometric information like fingerprints and iris scans, as other information was already available with public and private agencies in the country.[237] Right to privacy and confidentiality were sought to be protected by putting necessary provisions “in place”.[238] It was also observed in the context of privacy that loss of biometric information of a resident who is a victim of identity theft, especially when such information is linked to banking, social security and passport records, risks financial and other assets and the reputation of the resident.[239] According to the review, the envisaged UIDAI Act (which was still under contemplation at the time of publishing of this report and had not yet been legislated) would have remedies for the following offences:

[235] UIDAI, UIDAI Strategy Overview, available at http://www.prsindia.org/uploads/media/UID/UIDAI%20STRATEGY%20OVERVIEW. pdf, at page 4
[236] Ibid.
[237] Ibid, at page 32
[238] Ibid.
[239] Ibid, at page 33

- "Unauthorized disclosure of information by anyone in UIDAI, Registrar or the Enrolling agency;
- Disclosure of information violating the protocols set in place by UIDAI;
- Sharing any of the data on the database with anyone;
- Engaging in or facilitating analysis of the data for anyone;
- Engaging in or facilitating profiling of any nature for anyone or providing information for profiling of any nature for anyone;
- All offences under the Information Technology Act shall be deemed to be offences under UIDAI if directed against UIDAI or its database."[240]

However, according to the report, UIDAI was to concern itself only with identity fraud and any grievances in respect of document fraud (counterfeit/ misleading documents) were to be left to the Registrar enrolling the resident.[241]

141 The following conclusions emerge from the UIDAI's strategy overview: *Firstly*, the UIDAI was aware of the importance of biometric information before the Aadhaar programme had been rolled out. *Secondly*, UIDAI had itself contemplated a scenario of identity theft which could occur at the time of enrollment for Aadhaar cards. However, it had no solution to the possible harms which could result after the identity theft of a person, more so when the potential 'UIDAI Act' was still in the pipeline and was not eventually enacted until 2016.

[240] Ibid.
[241] Ibid, at page 34

C. Registrars

142 The term 'Registrar' was first defined by UIDAI in its DDSVPC Report as "*any government or private agency that will partner with UIDAI in order to enroll and authenticate residents*".[242] In the Strategy Overview, the term was defined as "*agencies such as central and state departments and private sector agencies who will be 'Registrars' for the UIDAI*".[243]

The Strategy Overview also stated that:

> "Registrars will process UID applications, and connect to the CIDR to de-duplicate resident information and receive UID numbers. These Registrars can either be enrollers, or will appoint agencies as enrollers, who will interface with people seeking UID numbers. The Authority will also partner with service providers for authentication. **If the Registrar issues a card to the resident,** the UIDAI will recommend that the card contain the UID number, name and photograph. **They will be free to add any more information related to their services (such as Customer ID by bank). They will also be free to print/ store the biometric collected from the applicant on the issued card.** If more registrars store such biometric information in a single card format, the cards will become interoperable for offline verification. **But the UIDAI will not insist on, audit or enforce this.**"[244] (Emphasis supplied)

143 In the 'Aadhaar Handbook for Registrars 2010' ("**2010 Handbook**"), following policy guidelines were laid down in respect of Registrars:

> 1. "Registrars may retain the biometric data collected from residents enrolled by them. However, the Registrar will have to exercise a fiduciary duty of care with respect to the data collected from residents and will be responsible for loss, unauthorized access to and misuse of data in their custody.
> 2. In order to ensure data integrity and security, the biometrics captured shall be encrypted upon collection by using the

[242] DDSVPC (UIDAI), DDSVPC Report, (9 December 2009), available at https://uidai.gov.in/images/UID_DDSVP_Committee_Report_v1.0. pdf , at page 5
[243] UIDAI, UIDAI Strategy Overview, available at http://www.prsindia.org/uploads/media/UID/UIDAI%20STRATEGY%20OVERVIEW.pdf, at page 2
[244] Ibid, at page 15

> encryption key defined by the Registrar. It is the responsibility of the Registrar to ensure the safety, security and confidentiality of this data which is in their custody. The Registrar must protect the data from unauthorized access and misuse. **The UIDAI will define guidelines for the storage of biometric data in order to give the Registrar some guidance on ensuring security of the data.** The Registrar shall have to define their own security policy and protocols to ensure safety of the Biometric data. The Registrars shall bear liability for any loss, unauthorized access and misuse of this data. **In the interest of transparency, it is recommended that the Registrar inform the resident that they will be keeping the biometric data and also define how the data will be used and how it will be kept secure."**[245] (Emphasis supplied)

In the 'Aadhaar Handbook for Registrars 2013' ("**2013 Handbook**"), it was stated that "***UIDAI has defined security guidelines for the storage of biometric data***".[246] While it is indicated in the handbook that guidelines for storage were defined by UIDAI, it is evident that this took place only after 2010 before which the registrars were functioning without guidelines mandating how the biometric data was to be kept secure.

The following guideline finds mention both in the Handbook of 2010 and 2013:

> "In the interest of transparency, it is recommended that the Registrar inform the resident that they will be keeping the biometric data and also define how the data will be used and how it will be kept secure".[247]

However, it is apparent from this guideline that it was merely a recommendation to the Registrars, and no obligation was cast upon the

---

[245] UIDAI, Aadhaar Handbook for Registrars, available at http://doitc.rajasthan.gov.in/administrator/Lists/Downloads/Attachments/26/aadhaar_handbook_version. pdf, at page 11

[246] Annexure R-74, Volume III, List of Pre-enactment dates and events for the Aadhaar project, Submissions by the AG.

[247] UIDAI (Planning Commission), Aadhaar Handbook for Registrars (2010), available at http://indiamicrofinance.com/wp-content/uploads/2010/08/Aadhaar-Handbook. pdf, at page 11; UIDAI (Planning Commission), Aadhaar Handbook for Registrars (2013), at page 16 (Annexure R-74, List of Pre-enactment dates and events for the Aadhaar project submitted by the Learned AG).

Registrars, to inform residents that their biometric data will be stored by them and how the data was to be used and kept secure. In contrast, Regulation 5 of the Aadhaar (Sharing of Information) Regulations 2016, states:

> **"Responsibility of any agency or entity** other than requesting entity with respect to Aadhaar number. —
>
> **(1) Any individual, agency or entity which collects Aadhaar number or any document containing the Aadhaar number, shall:** (a) collect, store and use the Aadhaar number for a lawful purpose; **(b) inform the Aadhaar number holder the following details:— i. the purpose for which the information is collected; ii. whether submission of Aadhaar number or proof of Aadhaar for such purpose is mandatory or voluntary, and if mandatory, the legal provision mandating it; iii. alternatives to submission of Aadhaar number or the document containing Aadhaar number, if any; (c) obtain consent of the Aadhaar number holder to the collection, storage and use of his Aadhaar number for the specified purposes.**
> (2) Such individual, agency or entity shall not use the Aadhaar number for any purpose other than those specified to the Aadhaar number holder at the time of obtaining his consent.
> (3) Such individual, agency or entity shall not share the Aadhaar number with any person without the consent of the Aadhaar number holder." (Emphasis supplied)

144 What the Registrar is obliged to do under law after the enactment of the Aadhaar Act, was a recommendation to the Registrar prior to the enactment of the Aadhaar Act. Thus, it is uncertain whether residents were informed about where and how their data would be kept secure since the guidelines to the Registrars were only recommendatory in nature. Similarly, in a UIDAI document titled 'Roles and Responsibilities of Enrollment Staff, 2017', one of the 'Fifteen Commandments that an Operator must remember during Resident Enrollment' is "*Make sure that the resident is well informed that his/her*

biometric will only be used for Aadhaar Enrolment/Update and no other purpose".[248] However, in the UIDAI document titled 'Enrollment Process Essentials, 2012', there is no mention of any such obligation being placed upon the enrolment staff.[249] In the absence of informed consent for the collection of data, a shadow of potential illegality is cast.

F.4 Privacy Concerns in the Aadhaar Act

1 Consent during enrolment and authentication & the right to access information under the Aadhaar Act

145 Section 3(2) of the Aadhaar Act requires enrolment agencies to inform the individual being enrolled about: a) the manner in which information shall be used; b) the nature of recipients with whom the information is to be shared during authentication; and c) the existence of a right to access information. However, the Enrolment Form in Schedule I of the Enrolment Regulations does not offer any clarification or mechanism on how the mandate of Section 3(2) is to be fulfilled.

The right of an individual to access information related to his or her authentication record is recognized in Section 3(2)(c) and Section 32(2) of the

[248] UIDAI, Roles and Responsibilities of Enrolment Staff, available at https://idai.gov.in/images/annexure_b_roles_and_responsibility_of_enrolment_staff._Pdf , at page 8

[249] UIDAI, Enrolment Process Essentials (13 December 2012), available at http://www.nictcsc.com/images/Aadhaar%20Project%20Training%20Module/English%20Training%20Module/module2_aadhaar_enrolment_process17122012. pdf

Aadhaar Act. However, the supplementary regulations that complement the Act are bereft of detail on the procedure to access such information.

Similarly, Regulation 9(c) of the Enrolment Regulations states that the procedure for accessing data would be provided to residents through the enrolment form, which is found in Schedule I to the Enrolment Regulations. However, all that Schedule I states is: "*I have a right to access my identity information (except core biometrics) following the procedure laid down by UIDAI"*, without any such procedure actually being laid down.

146 Section 2(l) of the Act, which defines an enrolling agency read with Regulation 23 of the Aadhaar (Enrolment and Update) Regulations allows for the collection of sensitive personal data (demographic and biometric information) of individuals by private agencies, which also have to discharge the burden of explaining the voluntary nature of Aadhaar registration and obtaining an individual's informed consent.

The Authentication Regulations, framed under sub-section (1), and sub-clauses (f) and (w) of sub-section (2) of Section 54 of the Aadhaar Act deal with the authentication framework for Aadhaar numbers, the governance of authentication agencies and the procedure for collection, storage of authentication data and records. Regulation 5 (1) states what details shall be made available to the Aadhaar number holder at the time of authentication

which are *a) the nature of information that will be shared by the Authority upon authentication, (b) the uses to which the information received during authentication may be put; and (c) alternatives to submission of identity information.* Regulation 6 (2) mandates that a requesting entity shall obtain the consent of an Aadhaar number holder for authentication in physical or, preferably, in electronic form and maintain logs or records of the consent obtained in the manner and form as may be specified by the Authority for this purpose.

Although Regulation 5 mentions that at the time of authentication, requesting entities shall inform the Aadhaar number holder of alternatives to submission of identity information for the purpose of authentication, and Regulation 6 mandates that the requesting entity shall obtain the consent of the Aadhaar number holder for the authentication, in neither of the above circumstances do the regulations specify the clearly defined options that should be made available to the Aadhaar number holder in case they do not wish to submit identity information, nor do the regulations specify the procedure to be followed in case the Aadhaar number holder does not provide consent. This is a significant omission. Measures for providing alternatives must be defined in all identity systems, particularly those that are implemented on a large scale.

2 Extent of information disclosed during authentication & sharing of core biometric information

147 Section 8(4) of the Act permits the Authority to respond to an authentication query with a "*positive, negative or any other appropriate response sharing such identity information excluding any core biometric information*". The petitioners have argued that the wide ambit of this provision gives the Authority discretion to respond to the requesting entity with information including an individual's photograph, name, date of birth, address, mobile number, email address and any other demographic information that was disclosed at the time of enrolment.

Moreover, it must be realized that even if core biometric information cannot be shared, demographic information is nonetheless, sensitive. Regulation 2(j) of the Authentication Regulations[250] provides that a digitally signed response with e-KYC data[251] [which is defined in Regulation 2(k)] can be returned to the requesting entity, while Regulation 3(ii)[252] provides for this form of authentication (e-KYC) by UIDAI.

[250] Regulation 2(j) of Aadhaar (Authentication) Regulations: "e-KYC authentication facility" means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction.

[251] Regulation 2(k) of Aadhaar Authentication Regulations: "e-KYC data" means demographic information and photograph of an Aadhaar number holder.

[252] Regulation 3(ii) of Aadhaar (Authentication) Regulations, 2016: "**3. Types of Authentication-There shall be two types of authentication facilities provided by the Authority, namely**— (i) Yes/No authentication facility, which may be carried out using any of the modes, (ii) e-KYC authentication facility, which may be carried out only using OTP and/ or biometric authentication modes as specified in regulation 4(2)".

148 Section 29(1) of the Aadhaar Act expressly states that '*core biometric information can never be shared with anyone for any reason whatsoever or be used for any purpose other than generation of Aadhaar numbers and authentication under this Act'.* However, this provision which seemingly protects an individual's core biometric information from being shared is contradicted by Section 29(4)[253] of the Act, the proviso to which grants UIDAI the power to publish, display or post core biometric information of an individual for purposes specified by the regulations. The language of this section is overbroad and which could lead to transgressions and abuse of power. Moreover, sub-sections 29(1) and (2), in effect, create distinction between two classes of information (core biometric information and identity information), which are integral to individual identity. Identity information requires equal protection as provided to core biometric information.

3 Expansive scope of biometric information

149 Definitions of biometric information [Section 2(g)], core biometric information [Section 2(j)] and demographic information [Section 2(k)] under the Aadhaar Act are inclusive and expansive. Section 2(g) defines 'biometric information' as "photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations". Section 2(j) defines 'core biometric information' as "*fingerprint, Iris scan, or such other*

[253] Section 29(4) states: "No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations."

biological attribute of an individual as may be specified by regulations". Section 2(t) explains that the regulations are to be made by UIDAI, which is the supreme authority under the Act. Sections 2(g), (j), (k) and (t) give discretionary power to UIDAI to define the scope of biometric and demographic information. Although the Act specifically provides what information can be collected, it does not specifically prohibit the collection of further biometric information. The scope of what can, in addition, be collected, has been left to regulations. These provisions empower UIDAI to expand on the nature of information already collected at the time of enrolment, to the extent of also collecting *'such other biological attributes*' that it may deem fit by specifying it in regulations at a future date.

The definitions of these sections provide the government with unbridled powers to add to the list of biometric details that UIDAI can require a citizen to part with during enrolment which might even amount to an invasive collection of biological attributes including blood and urine samples of individuals.

4 Other concerns regarding the Aadhaar Act: Misconceptions regarding the efficacy of biometric information

150 The uniqueness of a fingerprint in forensic science remains an assumption without watertight proof. The uniqueness of biometric data is not absolute, it is relative. Not everyone will have a particular biometric trait, or an individual's biometric trait may be significantly different from the 'normal'

expected trait. Some people may be missing fingerprints due to skin or other disease, which may cause further problems when enrolling a large population in a fingerprint-based register. Discrimination concerns may also be raised in such a case. Therefore, a large scale biometric scheme will usually need to utilise more than one biometric. For example- both fingerprint and face to ensure all people can be enrolled.[254]

The stability of even so called stable types of biometric data is not absolute. Each time an individual places a fingerprint on a fingerprint reader, the pattern may appear to be the same from a short distance, but there are actually small differences in the pattern due to dryness, moisture and elasticity of the skin. Moreover, cuts and scratches can alter the pattern. Similarly, even the iris, a popular biometric measurement suffers from difficulties in obtaining a valid image. The iris can also be hindered by specula reflections in uncontrolled lighting situations. These problems also apply to other relatively stable biometric identifiers.[255]

151 Sections 6[256] and 31(2)[257] of the Aadhaar Act place an additional onus on individual Aadhaar holders to update their information. These provisions

[254]Ramesh Subramanian, Computer Security, Privacy & Politics: Current Issues, Challenges & Solutions, IRM Press, at pages 99-100

[255]Ibid, at page 100

[256]Section 6 states: "The Authority may require Aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations, so as to ensure continued accuracy of their information in the Central Identities Data Repository."

[257]Section 31(2) states: "In case any biometric information of Aadhaar number holder is lost or changes subsequently for any reason, the Aadhaar number holder shall request the Authority to make necessary alteration in his record in the Central Identities Data Repository in such manner as may be specified by regulations."

create a legal mandate on individuals to ensure that their information is accurate within the CIDR. It is an acknowledgement that an individual's biometric information may change from time to time. Natural factors like ageing, manual labour, injury and illness can cause an individual's biometric information to be altered over the course of a lifetime. Critics of the Aadhaar program however point to the fact that provisions for updation fly in the face of UIDAI's repeated advertisements that Aadhaar enrolment is a "one-time" affair, as it is not and will never be. Moreover, there is no way in which a person can estimate that he or she is due for an update, as this is not something that can be discerned by actions as innocuous as looking in the mirror or at one's fingers, and therefore there remains no objective means of complying with the above sections. In fact, an authentication failure and a subsequent denial of welfare benefits, a subsidy or a service that an individual is entitled to might be the only way one comes to the conclusion that his or her biometrics need to be updated in the CIDR.[258]

Moreover, since the promise of Aadhaar as a unique identity hinges on the uniqueness of biometrics, it would be logical to assume that any update to biometric data should go through the same rigour as a new enrolment. Regulation 19(a), entitled 'Modes of Updating Residents Information' under Chapter IV of the Aadhaar (Enrolment and Update) Regulations, 2016 provides:

[258] L. Vishwanath, Four Reasons You Should Worry About Aadhaar's Use of Biometrics, The Wire (28 March, 2017), available at https://thewire.in/rights/real-problem-aadhaar-lies-biometrics

> "19. Mode of Updating Residents Information:
> a) At any enrolment centre with the assistance of the operator and/or supervisor. The resident will be biometrically authenticated and shall be required to provide his Aadhaar number along with the identity information sought to be updated."

This raises the question as to how an individual will update his/her biometric information. If the biometric information stored in CIDR has changed, the present biometrics will lead to mismatch during authentication. This Regulation does not provide any real clarity on how updation should be taking place in practice for the following reasons:

1. As required by the regulation, can an individual be asked to undergo biometric authentication, when the purpose is to update the biometrics?
2. Does the provision amount to an implied expectation that an individual is supposed to revisit the enrolment centre before all ten fingers and two irises (core biometric information) are rendered inaccurate for the purposes of authentication?[259]

This is also evidence of the fact that an Aadhaar enrolment is not a one-time affair.

5 No access to biometric records in database

152 The proviso to Section 28(5)[260] of the Aadhaar Act disallows an individual access to the biometric information that forms the core of his or her

[259] Ibid.
[260] Section 28(5) states: "Notwithstanding anything contained in any other law for the time being in force, and save as otherwise provided in this Act, the Authority or any of its officers or other employees or any agency

unique ID (Aadhaar). The lack of access is problematic for the following reasons: First, verification of whether the biometrics have been recorded correctly or not in the first place is not possible. This becomes critical when that same information forms the basis of identity and is the basis of authentication and subsequent access to welfare benefits and other services. Second, there is a great potential for fraudulently replacing a person's biometric identity in the database, as the individual has no means to verify the biometric information that has been recorded at the time of enrolment. Even an entity like the enrolment operator (with a software hack) could upload someone else's biometrics against another person.[261] Denial of access to the individual violates a fundamental principle of data protection: ownership of the data must at all times vest with the individual. Overlooking this fundamental principle is manifestly arbitrary and violative of Article 14.

6 Biometric locking

153 Authentication Regulations 11 (1) and (4) provide for the facility of Biometric Locking. Regulation 11(1) provides:

> "The Authority may enable an Aadhaar number holder to permanently lock his biometrics and temporarily unlock it when needed for biometric authentication."

---

that maintains the Central Identities Data Repository shall not, whether during his service or thereafter, reveal any information stored in the Central Identities Data Repository or authentication record to anyone:
Provided that an Aadhaar number holder may request the Authority to provide access to his identity information excluding his core biometric information in such manner as may be specified by regulations."

[261] L. Vishwanath, Four Reasons You Should Worry About Aadhaar's Use of Biometrics, The Wire (28 March, 2017), available at https://thewire.in/rights/real-problem-aadhaar-lies-biometrics

Regulation 11(4) provides:

> "The Authority may make provisions for Aadhaar number holders to remove such permanent locks at any point in a secure manner."

The provision allowing biometric locking is salutary to the extent that it allows Aadhaar number holders to permanently lock their biometrics and temporarily unlock them only when needed for biometric authentication. But the regulation is problematic to the extent that it also empowers the UIDAI to make provisions to remove such locking without any specified grounds for doing so.[262]

7 Key takeaways

154 The use of biometric technology is only likely to grow dramatically both in the private and public sector. On our part, we can only ensure that the strides made in technology are accompanied by stringent legal and technical safeguards so that biometrics do not become a threat to privacy.[263]

155 There is no unique concept of privacy and there maybe trade-offs between privacy and other objectives.[264] The challenge regarding privacy is best put in the following words:

[262] The Centre for Internet & Society, Analysis of Key Provisions of the Aadhaar Act Regulations, (31 March, 2017), available at https://cis-india.org/internet-governance/blog/analysis-of-key-provisions-of-aadhaar-act-regulations.

[263] A. Cavoukian, Privacy and Biometrics, Information and Privacy Commissioner Canada (1999), available at http://www.ipc.on.ca/images/Resources/pri-biom.pdf

[264] Robert Gellman. Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries, CGD Policy Paper 028 Washington DC: Centre for Global Development (1 August 2013), available at https://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0. pdf

> "The definition of privacy in any jurisdiction must take into account cultural, historical, legal, religious and other local factors. One size may not fit all countries, regions, or cultures when it comes to privacy or to some elements of privacy. In addition, views of privacy change as time passes and technology advances. However, different perspectives are not a barrier to evaluating privacy but a challenge."[265]

The relationship between biometrics and privacy is completely shaped by the design of the systems and the framework within which private and personal data is handled. Unfortunately, particularly in developing countries the adoption of biometrics has not been accompanied by an adequate discussion of privacy concerns.[266] Biometrics can also be a "staunch friend of privacy" when the technology is used for controlling access and to restrict unauthorized personnel from gaining access to sensitive personal information.[267] While evaluating privacy consequences of biometric technology, it is also important to bear in mind that there cannot be an assumption that current privacy protections which may be appropriate for the present state of technology will also be sufficient in the future.[268] Technology will continue to develop as will the need to develop corresponding privacy protections. Concerns around privacy and data protection will have to be addressed. "Fair Information Practices (FIPs), Privacy by Design (PbD), and Privacy Impact Assessments (PIAs)"[269] might be useful in addressing these concerns. FIPs offer the substantive content for a privacy policy. PbD offers a proactive approach to

[265] Ibid
[266] Ibid
[267] John D Woodward, Biometrics: Identifying Law & Policy Concerns, in Biometrics (AK Jain A.K, R Bolle, and S Pankanti eds.), Springer (1996)
[268] Robert Gellman, Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries, CGD Policy Paper 028 Washington DC: Centre for Global Development (1 August, 2013), available at https://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0.pdf
[269] Ibid

the protection of privacy that relies on advance planning rather responding to problems after they arise. PIAs offer a formal way to consider and assess the privacy consequences of technology or other choices, including consideration of alternatives early in the planning stages. These three methodologies are not mutually exclusive and can be combined to achieve the just and optimal result for society.[270]

156 Of particular significance is the “Do Not Harm” principle which means that biometrics and digital identity should not be used by the issuing authority, typically a government, or adjacent parties to serve purposes that could harm the individuals holding the identification.[271] Identity systems, whether in paper or digital, must work for the public good and must do no harm. However, identity systems due to their inherent power, can cause harm when placed into hostile hands and used improperly. Great care must be taken to prevent this misuse. “Do No Harm” requires rigorous evaluation, foresight, and continual oversight.[272]

157 There are many adversarial actors – from private espionage groups to foreign governments, who may try to exploit data vulnerabilities. There is also the threat of abuse of power by future governments. However, creating and instilling strong privacy protection laws and safeguards may decrease these

[270] Ibid
[271] Pam Dixon, A Failure to Do No Harm – India’s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S., Health and Technology, Vol. 7 (2017), at pages 539–567
[272] Ibid

risks- such as the framework provided by the EUGDPR[273]. In order to uphold democratic values, the government needs to curtail its own powers concerning the tracking of all citizens and prevent the needless collection of data. Such protections may assuage the fears and uphold the long-term legitimacy of Aadhaar. If the legislative process takes into account public feedback and addresses the privacy concerns regarding Aadhaar, it would provide a solid basis for more digital initiatives, which are imminent in today's digital age. However, in its current form, the Aadhaar framework does not address the privacy concerns issues discussed in this section of the judgment.

G Legitimate state aim

G.I Directive Principles

158 The Union government has contended that the legitimate state interest in pursuing the Aadhaar project flows from the solicitous concern shown in the text and spirit of the Constitution for realising socio-economic rights. The right to food must, according to the view proposed before the Court, trump over the right to privacy. The Aadhaar project, it has been urged, seeks to fulfil socio-economic entitlements.

159 The Constituent Assembly did not work in a vacuum. The idealism with which the members of the Assembly drafted the Constitution was the result of

[273] General Data Protection Regulation, available at https://gdpr-info.eu/

the "social content of the Independence movement"[274], which came from the awareness of the members about the existing conditions of the Indian masses. Granville Austin has therefore referred to the Constitution as a "social document" and a "modernizing force", whose provisions reflect "humanitarian sentiments".[275] The Constitution was the medium through which the nascent Indian democracy was to foster many goals. Austin observes:

> "Transcendent among [the goals] was that of social revolution. **Through this revolution would be fulfilled the basic needs of the common man, and, it was hoped, this revolution would bring about fundamental changes in the structure of Indian society.**"[276] (Emphasis supplied)

Austin has further observed:

> "The first task of [the] Assembly… [was] to free India through a new constitution, to feed the starving people, and to clothe the naked masses, and to give every Indian the fullest opportunity to develop himself according to his capacity."[277]

In his work titled "The Constitution of India: A Contextual Analysis", Arun K Thiruvengadam identified one such goal of the Constitution as follows:

> "The Indian Constitution sought to lay the blueprint for economic development of the vast subcontinental nation, which was an imperative for a populace that was largely illiterate, poor and disproportionately situated in rural societies that had limited access to many essential social goods and infrastructural facilities.[278]"
>
> .
>
> "By establishing these positive obligations of the state, the members of the Constituent Assembly made it the responsibility of future Indian governments **to find a middle way between individual liberty and the public good,**

[274] Granville Austin, The Indian Constitution: Cornerstone of a Nation, Oxford University Press (1999) at page xxii
[275] Ibid, at pages 62, xiii and xxii
[276] Ibid, at page xxi
[277] Ibid, at page 32
[278] Arun K Thiruvengadam, The Constitution of India: A Contextual Analysis, (Bloomsbury 2017), at page 1

> **between preserving the property and the privilege of the few and bestowing benefits on the many in order to liberate 'the powers of all men equally for contributions to the common good'**."[279] (Emphasis supplied)

160 The draftpersons of the Constitution believed that the driving force to bring social change rested with the State. This is evident from an instance during the proceedings of the Constituent Assembly. Dr. B R Ambedkar had submitted to the Assembly a social scheme to be incorporated into the Constitution, which included provisions to cover every adult Indian by life insurance. However, his social scheme was rejected on the ground that such provisions should be left to legislation and need not be embodied into the Constitution.[280]

161 The social and economic goals which were contemplated at the time of Independence remain at the forefront of the State's agenda even today. Certain parts of the Constitution play a leading role in declaring the blueprint of its social intent. Directive Principles were specifically incorporated into the Constitution for this purpose. Though not enforceable in courts, the principles are "fundamental in the governance of the country" and it is the duty of the State to apply these principles while making laws.[281] The essence of the Directive Principles lies in Article 38 of the Constitution, which places an obligation on the State to secure a social order for the promotion of the

[279] Granville Austin, The Indian Constitution: Cornerstone of a Nation, Oxford University Press (1999) at page 66
[280] Ibid, at page 99
[281] Article 37, The Constitution of India

welfare of the people. Titled as Part IV of the Constitution, the Directive Principles are symbolic of the welfare vision of the Constitution makers.

Article 38 of the Constitution provides that :

> "(1) The State shall strive to promote the welfare of the people by securing and protecting as effectively as it may a social order in which justice, social economic and political, shall inform all the institutions of the national life.
>
> (2) The State shall, in particular, strive to minimize the inequalities in income, and endeavor to eliminate inequalities in status, facilities and opportunities, not only amongst individuals but also amongst groups of people residing in different areas or engaged in different vocations."

Clauses (b), (c), (e) and (f) of Article 39 provide thus :

> "39. The State shall, in particular, direct its policy towards securing -
>
> ...
>
> (b) that the ownership and control of the material resources of the community are so distributed as best to subserve the common good;
>
> (c) that the operation of the economic system does not result in the concentration of wealth and means of production to the common detriment;
>
> ..
>
> (e) that the health and strength of workers, men and women, and the tender age of children are not abused and that citizens are not forced by economic necessity to enter avocations unsuited to their age or strength;
>
> (f) that children are given opportunities and facilities to develop in a healthy manner and in conditions of freedom and dignity and that childhood and youth are protected against exploitation and against moral and material abandonment."

Article 41 speaks of the right to work, to education, and to public assistance :

> "41. The State shall, within the limits of its economic capacity and development, make effective provision for securing the right to work, to education and to public assistance in cases

> of unemployment, old age, sickness and disablement, and in other cases of undeserved want."

Article 43 contemplates a living wage and conditions of work which provide a decent standard of life:

> "43. The State shall endeavour to secure, by suitable legislation or economic organisation or in any other way, to all workers, agricultural, industrial or otherwise, work, a living wage, conditions of work ensuring a decent standard of life and full enjoyment of leisure and social and cultural opportunities and, in particular, the State shall endeavour to promote cottage industries on an individual or co-operative basis in rural areas."

Article 47 casts a positive obligation upon the State to raise the level of nutrition and the standard of living and to improve public health, as among its primary duties. Reflecting a constitutional vision of socio-economic justice, the values adopted in the Directive Principles are to be progressively realised in the course of social and economic development.

162 In a recently published book titled "Supreme Court of India: The Beginnings", George H Gadbois, Jr. observes that the Indian Constitution, "easily the lengthiest fundamental law in the world, probably ranks also as one of the most eclectic ever produced".[282] Reflecting upon the constitutional models from which the draftspersons of India's Constitution drew sustenance, Gadbois states:

> "The Constitution makes provision for a parliamentary system adapted from the British model, a federation patterned after the Government of India Act of 1935 and the Canadian

[282] George H Gadbois, JR, Supreme Court of India: The Beginnings (Vikram Raghavan and Vasujith Ram eds.), Oxford University Press (2017), at page 193

> Constitution, a set of emergency powers similar to those set forth in the Weimar Constitution, a lengthy list of fundamental rights adapted from the American experience with a Bill of Rights, a Supreme Court endowed with express powers of judicial review for which the American Supreme Court served as the model, and list of "Directive Principles of State Policy" patterned after the Constitution of Eire."[283]

Reflecting on the Directive Principles, Gadbois observes:

> "Suffice to say that the directive principles have provided the constitutional basis and justification for the Government's efforts to establish a welfare state, or, to use the designation preferred by Indian leaders, a "socialist pattern of society".[284]

The sanction behind the Directives, according to him "is political and not juridical". On the other hand, the fundamental rights are justiciable because Article 13 provides that a law which takes them away or abridges them will be void. The conflict as Gadbois sees it is this:

> "the directive principles are a set of instructions to the Government of the day to legislate into being a welfare state, which means, of course, an emphasis on the social and economic uplift of the community at large and a corresponding subtraction from individual rights. It is the duty of the Government to apply these principles in making laws. In short, the Constitution confers upon the Supreme Court the task of making the fundamental rights meaningful against possible infringements by the legislatures and executives, and makes it obligatory for the Government to bring about changes in the social and economic life of the nation, changes which were bound to affect adversely some private rights.
>
> It is conceivable at least, that both the Supreme Court and the Government could have pursued their respective tasks without conflict, but this did not happen. The legislatures, purporting to be doing no more than carrying out the duties prescribed in the directive principles, enacted legislation which the Supreme Court found to be in conflict with some of the fundamental rights."[285]

[283] Ibid, at pages 193-194
[284] Ibid, at page 195
[285] Ibid, at pages 195-196

This formulation by Gadbois formed part of a dissertation in **April 1965**. The evolution of jurisprudence in India since then has altered the Constitutional dialogue. Over time, the values enshrined in the Directive Principles have been read into the guarantees of freedom in Part III. In incremental stages, the realisation of economic freedom has been brought within the realm of justiciability, at least as a measure of the reasonableness of legislative programmes designed to achieve social welfare.

163 As our constitutional jurisprudence has evolved, the Directive Principles have been recognised as being more than a mere statement of desirable goals. By a process of constitutional interpretation, the values contained in them have been adopted as standards of reasonableness to expand the meaning and ambit of the fundamental rights guaranteed by Part III of the Constitution.[286] In doing so, judicial interpretation has attempted to imbue a substantive constitutional content to the international obligations assumed by India in the Universal Declaration of Human Rights and the International Covenant on Economic and Social and Cultural Rights. Eradicating extreme poverty and hunger is a significant facet of the Millennium Development Goals of the United Nations. Social welfare legislation is but a step to achieve those goals. The enactment of the National Food Security Act 2013 constituted a milestone in legislative attempts to provide food security at the household level. The Act discerns a targeted Public Distribution System for providing food-grains to those below the poverty line. The rules contemplated in Section

[286] Minerva Mills Ltd. v Union of India, (1980) 3 SCC 625

12(2)(b), incorporate the application of Information and Communication Technology tools to ensure transparency of governance and prevent a diversion of benefits. Another important piece of legislation has been the Mahatma Gandhi National Rural Employment Guarantee Act (MGNREGA) Act 2005 which was enacted for the enhancement of livelihood and security of rural households. The Act guarantees a hundred days of wage employment in every financial year to at least one able-bodied member of every household in rural areas in public works programmes designed to create public assets. Both the National Food Security Act 2013 and the MGNREGA Act 2005 follow a rights-based approach in dealing with endemic problems of poverty and deprivation in rural areas. Leveraging Aadhaar for biometric identification of beneficiaries, it has been argued by the respondents, is an intrinsic part of the legislative effort to ensure that benefits in terms of food security and employment guarantee are channelised to those for whom they are meant.

G.2 Development and freedom

164 Many scholars have delved into the substantive themes of the Indian Constitution. Upendra Baxi has argued that the Indian Constitution has four sovereign virtues: "rights, justice, development, and governance"[287]. Baxi notes that they are "intertwined and interlocked with the rest and, in contradictory combination/recombinations with both the constitutional and

[287]Upendra Baxi, "A known but an indifferent judge": Situating Ronald Dworkin in contemporary Indian jurisprudence, International Journal of Constitutional Law, (2003) at page 582

social past and their future images".[288] Development is a leading aspect of our constitutional vision. Development in the constitutional context is not only economic development assessed in terms of conventional indicators such as the growth of the gross domestic product or industrial output. The central exercise of development in a constitutional sense is addressing the "deprivation, destitution and oppression"[289] that plague an individual's life.

165 In a traditional sense, freedom and liberty mean an absence of interference by the state into human affairs. Liberty assumes the character of a shield. The autonomy of the individual is protected from encroachment by the state. This formulation of political rights reflects the notion that the state shall not be permitted to encroach upon a protected sphere reserved for individual decisions and choices. What the state is prevented from doing is couched in a negative sense. Civil and political rights operate as restraints on state action. They postulate a restriction on the state. Isaiah Berlin formulates the negative conception of liberty thus:

> "I am … free to the degree to which no man or body of man interferes with my activity. Political liberty is simply the area within which a man can act unobstructed by others."[290]

166 Individual freedom, in this conception, imposes a duty of restraint on the state. Modern ideas of neo liberalism have funnelled this notion. Neo-liberalism postulates that the increasing presence of the state is a threat to

[288] Ibid
[289] Amartya Sen, Development as Freedom, Oxford University Press (2000), at page xii
[290] Isaiah Berlin, Two Concepts of Liberty, available at http://faculty.www.umb.edu/steven.levine/courses/Fall%202015/What%20is%20Freedom%20Writings/Berlin.pdf

individual autonomy. A free market economy with minimum state control, in this view, is regarded as integral to protecting individual rights and freedoms. FA Hayek construes the content of liberty as meaning the absence of obstacles. Resultantly, this notion of liberty regards the role of the state in a narrow jurisprudential frame. Attempts by the state to pursue social justice or to use its authority for redistribution of wealth would in this conception not be a legitimate use of state power.[291]

167 The notion that liberty only consists of freedom from restraint does not complete the universe of its discourse. Broader notions of liberty are cognizant of the fact that individuals must be enabled to pursue their capacities to the fullest degree. Social and economic discrimination poses real barriers to access education, resources and the means to a dignified life. This approach to understanding the content of freedom construes the ability to lead a dignified existence as essential to the conception of liberty and freedom. The integral relationship between removal of socio-economic inequality and freedom has been eloquently set out by Amartya Sen in "Development as Freedom"[292]:

> "Development requires the removal of major sources of unfreedom: poverty as well as tyranny, poor economic opportunities as well as systematic social deprivation, neglect of public facilities as well as intolerance or overactivity of repressive states. Despite unprecedented increases in overall opulence, the contemporary world denies elementary freedoms to vast numbers – perhaps even the majority-of people. Sometimes the lack of substantive freedoms relates directly to economic poverty, which robs people of the

[291] F A Hayek, The Constitution of Liberty, Routledge & Kegan Paul, (1960) at pages 11, 207-208
[292] Amartya Sen, Development as Freedom, Oxford University Press (2000) at page 3-4

> freedom to satisfy hunger, or to achieve sufficient nutrition, or to obtain remedies for treatable illnesses, or the opportunity to be adequately clothed or sheltered, or to enjoy clean water or sanitary facilities. In other cases, the unfreedom links closely to the lack of public facilities and social care, such as the absence of epidemiological programs, or of organized arrangements for health care or educational facilities, or of effective institutions for the maintenance of local peace and order. In still other cases, the violation of freedom results directly from a denial of political and civil liberties by authoritarian regimes and from imposed restrictions on the freedom to participate in the social, political and economic life of the community."

In Sen's analysis, human development is influenced by economic opportunities, political liberties, social powers, and the enabling conditions of good health, basic education, and the encouragement and cultivation of initiatives. Taking it further, Sen has recognized an important co-relation in terms of the non-availability of basic economic conditions:

> "Economic unfreedom, in the form of extreme poverty, can make a person a helpless prey in the violation of other kinds of freedom… Economic unfreedom can breed social unfreedom, just as social or political unfreedom can also foster economic unfreedom."[293]

168 The notion of freedom as an agency has been developed by Sen as part of the 'capability theory'. The necessary consequence of focusing upon major sources of unfreedom, in a social and economic perspective, is that the removal of these restraints is essential to the realization of freedom. If true freedom is to be achieved through the removal of conditions which cause social and economic deprivation, the role of the state is not confined to an absence of restraint. On the contrary, the state has a positive obligation to

[293] Ibid, at page 8

enhance individual capabilities. Martha Nussbaum[294] argues that realising freedom requires the state to discharge positive duties. Nussbaum expresses a threshold level of capability below which true human functioning is not available. Freedom is seen in terms of human development and is the process by which individuals can rise above capability thresholds. In the realisation of basic rights, the state is subject to positive duties to further the fulfilment of freedom.

169 The broader conception of freedom and liberty which emerges from the writings of Sen and Nussbaum has direct consequences upon how we view civil and political rights and socio-economic rights. The distinction between the two sets of rights becomes illusory once civil and political rights are regarded as comprehending within their sweep a corresponding duty to take such measures as would achieve true freedom. Henry Shue[295] suggests that rights give rise to corresponding duties. These duties include:

(i) a duty to respect;
(ii) a duty to protect; and
(iii) a duty to fulfil.

Duties of **respect** embody a restraint on affecting the rights of others. Duties to **protect** mandate that the state must restrain others in the same manner as it restrains itself. The state's duty of non-interference extends to private individuals. The duty to **fulfil** connotes aiding the deprived in the realisation of

[294] Martha Nussbaum, Women and Human Development, Cambridge University Press, (2000)
[295] Henry Shue, Basic Rights: Subsistence, Affluence and US Foreign Policy, Princeton University Press, Second Edition (1996)

rights. This imposes a corresponding duty to create the conditions which will facilitate the realisation of the right. The right which is protected for the individual will also signify an expectation that the state must create institutions enabling the exercise of facilitative measures or programmes of action, of an affirmative nature. The state has affirmative obligations to fulfil in the realisation of rights. These positive duties of the state are readily apparent in the context of welfare entitlements when the state must adopt affirmative steps to alleviate poverty and the major sources of economic and social non-freedom. But the thesis of Nussbaum and Shue have an important role for the state to discharge in ensuring the fulfilment of political rights as well. In a highly networked and technology reliant world, individual liberty requires the state to take positive steps to protect individual rights. Data protection and individual privacy mandate that the state put in place a positive regime which recognises, respects and protects the individual from predatory market places. The state has a positive duty to create an autonomous regulatory framework in which the individual has access to remedies both against state and non-state actors, both of whom pose grave dangers of assault on the individual as an autonomous entity. Failure to discharge that duty is a failure of the state to respect, protect and fulfil rights.

Dr Ambedkar's prophetic final address to the Constituent Assembly elaborates that vision:

> "On the social plane, we have in India a society based on the principle of graded inequality with elevation for some and degradation for others. On the economic plane, we have a society in which there are some who have immense wealth as against many who live in abject poverty. On the 26th of

> January 1950, we are going to enter into a life of contradictions. In politics we will have equality and in social and economic life we will have inequality...How long shall we continue to live this life of contradictions? How long shall we continue to deny equality in our social and economic life? If we continue to deny it for long, we will do so only by putting our political democracy in peril. We must remove this contradiction at the earliest possible moment or else those who suffer from inequality will blow up the structure of political democracy which [this] Assembly has [so] laboriously built up."[296]

The pursuit of social welfare and security is a central aspect of development. The State, in Ambedkar's vision, would be the main instrumentality in the debate on development, which has to revolve around the social, economic and political spheres and would be guided by the values of the Constitution.

170 Social opportunities are the facilities and "arrangements that society makes" for education, healthcare and nutrition, which "influence the individual's substantive freedom to live better".[297] Social security measures include programmes which intend to promote the welfare of the population through assistance measures guaranteeing access to sufficient resources. The social security framework is not only important for individual development, but also for effective participation in economic and political activities. Social security programmes flow from 'economic and social rights'– also called as "welfare rights" [298] or second generation rights. These rights, recognized for the first time under the Universal Declaration on Human Rights, 1948 include a large list of freedoms and claims under its "protective

[296] Constituent Assembly Debates (25 November 1949)
[297] Amartya Sen, Development as Freedom, Oxford University Press (2000), at page 39
[298] Amartya Sen, The Idea of Justice, Penguin (2009) at pages 379-380

umbrella". They include not only basic political rights, but the right to work, the right to education, protection against unemployment and poverty, the right to join trade unions and even the right to just and favourable remuneration.[299] Social security programmes as an instrument for the removal of global poverty and other economic and social deprivations are at the centre stage in the global discourse. Article 22 of the Universal Declaration of Human Rights expressly recognises that every member of society is entitled to the right to social security and to the realisation of economic, social and cultural rights. Those rights are stated to be indispensable for dignity and to the free development of personality. The realisation of these rights has to be facilitated both through national efforts and international co-operation and in accordance with the organisation and the resources of each state. Article 22 stipulates that:

> "Article 22
> Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality."

In a similar vein, Article 23 comprehends a conglomeration of rights including (i) the right to work; (ii) free choice of employment; (iii) just and favourable conditions of work; (iv) protection against unemployment; (v) equal pay for equal work without any discrimination; (vi) just and favourable remuneration for work; and (vii) formation and membership of trade unions. Article 23

[299] Ibid, at page 380

construes these rights as a means of ensuring both for the individual and the family, an “existence worthy of human dignity” supplemented if necessary “by other means of social protection”.

India having adopted the UDHR, its principles can legitimately animate our constitutional conversations. Both Articles 22 and 23 are significant in recognising economic rights and entitlements in matters of work and social security. Both the articles recognise the intrinsic relationship between human dignity and the realisation of economic rights. Measures of social protection are integral to the realisation of economic freedom and to fulfil the aspiration for human dignity.

171 India adopted and ratified the Covenant on Civil and Political Rights as well as the Covenant on Economic, Social and Cultural Rights. India acceded to the Covenant on Economic, Social and Cultural Rights on 10 April 1979. According to the Preamble, the states who are parties to the Covenant have recognized that:

> “the ideal of free human beings enjoying freedom from fear and want can only be achieved if conditions are created whereby everyone may enjoy his economic, social and cultural rights, as well as his civil and political rights.”

Freedom is thus defined in terms of the absence of fear and want. Moreover, freedom consists in the enjoyment of a conglomeration of rights: economic,

social and cultural as well as civil and political rights. There is in other words no dichotomy between the two sets of rights.

Article 11 of the Covenant on Economic, Social and Cultural Rights imposes positive obligations on the covenanting states:

> "Article 11.
> 1. The States Parties to the present Covenant recognize the right of everyone to an adequate standard of living for himself and his family, including adequate food, clothing and housing, and to the continuous improvement of living conditions. The States Parties will take appropriate steps to ensure the realization of this right, recognizing to this effect the essential importance of international cooperation based on free consent.
>
> 2. The States Parties to the present Covenant, recognizing the fundamental right of everyone to be free from hunger, shall take, individually and through international co-operation, the measures, including specific programmes, which are needed:
>
> (a) To improve methods of production, conservation and distribution of food by making full use of technical and scientific knowledge, by disseminating knowledge of the principles of nutrition and by developing or reforming agrarian systems in such a way as to achieve the most efficient development and utilization of natural resources;
> (a) Taking into account the problems of both food-importing the food-exporting countries, to ensure an equitable distribution of world food supplies in relation to need."

172 The Masstricht Guidelines on Violations of Economic, Social and Cultural Rights (January 1997) stipulate that:

> "It is now undisputed that all human rights are indivisible, interdependent, interrelated and of equal importance for human dignity. Therefore, states are as responsible for violations of economic, social and cultural rights as they are for violations of civil and political rights."

The Guidelines also stipulate that like civil and political rights, economic, social and cultural rights impose three different types of obligations on states : the obligation to respect, protect and fulfil. The guidelines recognize that violations of economic, social and cultural rights can occur through acts of commission and omission on the part of states. The omission or failure of states to take measures emanating from their legal obligations may result in such violations. Among them is the failure to enforce legislation or to put into effect policies designed to implement the provisions of the Covenant. In similar terms, the Limburg Principles on the Implementation of the International Covenant on Economic, Social and Cultural Rights cast affirmative duties on states to take immediate steps towards realizing the rights contained in the Covenant. Clauses 16, 21 and 27 of the guidelines are thus:

> "16. All States parties have an obligation to begin immediately to take steps towards full realization of the rights contained in the Covenant.
> 21. The obligation "to achieve progressively the full realization of the rights" requires States parties to move as expeditiously as possible towards the realization of the rights. Under no circumstances shall this be interpreted as implying for States the right to defer indefinitely efforts to ensure full realization. On the contrary all States parties have the obligation to begin immediately to take steps to fulfil their obligations under the Covenant.
> 27. In determining whether adequate measures have been taken for the realization of the rights recognized in the Covenant attention shall be paid to equitable and effective use of and access to the available resources."

The office of the UN High Commissioner for Human Rights notified General Comment No. 3, which was adopted at the fifth session of the Committee on

Economic, Social and Cultural Rights on 14 December 1990. The Comment states:

> "…while the full realization of the relevant rights may be achieved progressively, steps towards that goal must be taken within a reasonably short time after the Covenant's entry into force for the States concerned. Such steps should be deliberate, concrete and targeted as clearly as possible towards meeting the obligations recognized in the Covenant."

Similarly, General Comment No. 12 on the right to adequate food was adopted at the twentieth session of the Committee on Economic, Social and Cultural Rights on 12 May 1999. It states :

> "The Committee observes that while the problems of hunger and malnutrition are often particularly acute in developing countries, malnutrition, under-nutrition and other problems which relate to the right to adequate food and the right to freedom from hunger also exist in some of the most economically developed countries, Fundamentally, the roots of the problem of hunger and malnutrition are not lack of food but lack of access to available food, inter alia because of poverty, by large segments of the world's population."

The emphasis on the lack of **access** to available food is significant to the present discourse. It indicates that access to food requires institutional mechanisms to ensure that the available resources reach the beneficiaries for whom they are intended.

173 Section 2(1)(f) of the Protection of Human Rights Act 1993 specifically adverts to the Covenant on Economic, Social and Cultural Rights:

> "2.(1)(f) "International Covenants" means the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights adopted by the General Assembly of the United Nations on 16th December, 1996 and such other Covenant or Convention

> adopted by the General Assembly of the United Nations as the Central Government may, by notification, specify;"

Under Section 12(f), the National Human Rights Commission has been entrusted with the function of studying treaties and other international instruments of human rights and to make recommendations for their effective implementation. Parliament has statutorily incorporated India's obligations at international law under the above covenants as a part of the national effort to realise fundamental human freedoms. Achieving economic freedom is integral to that mission**.** In his classic work "The Idea of Justice", Amartya Sen has observed in this regard:

> "The inclusion of second-generation rights makes it possible to integrate ethical issues underlying general ideas of global development with the demands of deliberative democracy, both of which connect with human rights and quite often with an understanding of the importance of advancing human capabilities."[300]

174 Social security thus acts as an underpinning link with development. There is also a two-way relationship between development and social security (expansion of human capability). Dreze and Sen have dealt with this relationship in their following observation:

> "Growth generates resources with which public and private efforts can be systematically mobilized to expand education, health care, nutrition, social facilities, and other essentials of fuller and freer human life for all. And the expansion of human capability, in turn, allows a faster expansion of resources and production, on which economic growth ultimately depends… Well-functioning public services, especially (but not only) in fields such as education and health, are also critical in fostering participatory growth as well as in ensuring that

[300] Amartya Sen, The Idea of Justice, Penguin (2009) at page 381

> growth leads to rapid improvements in people's living conditions."[301]

The authors have further observed that apart from education and healthcare, India faces larger issues of accountability in the "public sector as a whole".[302] The lack of progress in public services acts as a huge barrier to improve the quality of life of people.[303] It has been observed:

> "The relative weakness of Indian social policies on school education, basic healthcare, child nutrition, essential land reform and gender equity reflects deficiencies of politically engaged public reasoning and social pressure, not just inadequacies in the official thinking of the government."[304]

The future of Indian democracy therefore depends on how it engages itself with the issues of accountability in transfer of basic human facilities to the common man.

175 The State has a legitimate aim to ensure that its citizens receive basic human facilities. In order to witness development, the huge amount of expenditure that the State incurs in providing subsidies and benefits to the common citizens, must be accompanied by accountability and transparency. Legislative and institutional changes are often capable of creating an atmosphere of transparency and accountability. The most visible example of a legislative enactment which brought institutional changes is the Right to Information Act, 2005. Commentators have often highlighted the importance

[301] Jean Dreze and Amartya Sen, An Uncertain Glory, Penguin (2013), at pages x and xi
[302] Ibid, at page xi
[303] Jean Dreze and Amartya Sen, An Uncertain Glory, Penguin (2013), at page 33
[304] Amartya Sen, The Idea of Justice, Penguin (2009) at page 349

of this legislation by deliberating upon how it has been successful at "curbing corruption and restoring accountability in public life"[305]. According to the State, though the Aadhaar programme is not in itself a social security programme, the institutional framework established by the Act, seeks to act, in a way, as an extension of social security programmes. The State has a legitimate concern to check that the welfare benefits which it marks for those, who are entitled, reach them without diversion. The Aadhaar programme, it is argued, acts as an instrument for the realization of the benefits arising out of the social security programmes. The Aadhaar programme, it was further contended, fulfils the State's concern that its resources are utilised fully for human development.

It has been contended by the Respondents that since the establishment of the UIDAI in 2009, its basic mandate is to provide a unique identity number to residents. The number would subserve two purposes. First, it would serve as a proof of identity. Second, it would be used for the purpose of identifying beneficiaries for the transfer of social welfare benefits, provided by the state. The rationale for establishing a method of identification is to ensure that the benefits provided by social welfare programmes formulated by the State reach the beneficiaries for whom they are intended. As a policy intervention, a unique measure of identification is intended, it has been argued, to secure financial inclusion. A significant hurdle in the success of social welfare programmes is that benefits do not reach the targeted population. The reason

[305] Jean Dreze and Amartya Sen, An Uncertain Glory, Penguin (2013), at page 100

for this may have something to do intrinsically with the condition of the individuals as much as with their larger socio-economic circumstances. Migrant labour and labour in the unorganised sector lacks fixity of abode. The nature of their work renders their lives peripatetic. Nomadic tribes, particularly in inaccessible areas, may not have fixed homes. In many cases, traditional occupations require individuals to move from place to place, dependent on seasonal changes. Then again, groups of citizens including women, children and the differently abled may face significant difficulties in accessing benefits under publicly designed social welfare programmes as a result of factors such as gender, age and disability.

176 Unequal access to welfare benefits provided by the State becomes a significant source of deprivation resulting in a denial of the means to sustain life and livelihood. Before the adoption of Aadhaar based-identity, there were multiple platforms for identification of residents. They created a situation where those with no identity had no access to the means of sustaining a dignified life. Equally significant, as a policy intervention, was the issue of capture. While on the one hand, large swathes of the population had no access to welfare assistance, benefits could be captured by persons not entitled to them either by the assertion of fake or multiple identities. Setting up a fake identity enables an individual to pass off as another and to secure a benefit to which that individual is not entitled. Fake identities compound the problem of capture by allowing individuals to receive multiple benefits through

shell identities. Policy makers were confronted with the serious problems posed by fake and multiple identities since they imposed a burden on the exchequer while at the same time diluting the efficacy of state designed social welfare measures. The burden on the exchequer is illustrated by situations where persons who are not entitled to benefits secure them in the guise of being persons entitled to them. When imposters secure benefits which are not meant for them, they deprive in the process, persons who are genuinely entitled to benefits. The class of beneficiaries of social welfare programmes is, so to speak, adulterated by the capture of benefits by those not entitled to them. This raises serious concerns of the deprivation of human rights. The capture of benefits has the consequence of depriving those to whom these benefits should legitimately flow, of the measures designed by the state to protect its populace from human want and need. The resources deployed by the state are from its public revenues. When designing a unique measure of identification, the state must be guided by the necessity of ensuring financial inclusion and of protecting against financial exclusion. Every citizen who is eligible for social welfare benefits should obtain them. No person who is entitled should be excluded. Individuals who do not qualify for social welfare benefits should not capture them by passing off as individuals entitled. Enforcing and implementing a robust platform for identification of beneficiaries must ensure that social welfare benefits reach the hands of those who fulfil the conditions of eligibility and are not captured by rent-seeking behaviour of those to whom social welfare benefits are not designed. This constitutes a

legitimate object of state policy. Reaching out to the targeted population is a valid constitutional purpose. Social welfare measures are an intrinsic part of state policy designed to facilitate dignified conditions of existence to the marginalised, especially those who live below the poverty line. Identification of beneficiaries is crucial to the fulfilment of social welfare programmes.

177 These concerns form the basis of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016. As its Statement of Objects and Reasons explains:

> "The correct identification of targeted beneficiaries for delivery of various subsides, benefits, services, grants, wages and other social benefits schemes which are funded from the Consolidated Fund of India has become a challenge for the Government. The failure to establish identity of an individual has proved to be a major hindrance for successful implementation of these programmes. This has been a grave concern for certain categories of persons, such as women, children, senior citizens, persons with disabilities, migrant unskilled and unorganised workers, and nomadic tribes. In the absence of a credible system to authenticate identity of beneficiaries, it is difficult to ensure that the subsidies, benefits and services reach to intended beneficiaries."

The Statement of Objects and Reasons indicates that the enactment is designed to ensure "the **effective, secure and accurate** delivery of benefits, subsidies and services from the Consolidated Fund of India to targeted beneficiaries". The architecture of the law contemplates regulating the following aspects:

> "(a) issue of Aadhaar numbers to individuals on providing .. demographic and biometric information to the Unique Identification Authority of India;
> (b) requiring, Aadhaar numbers for identifying an individual for delivery of benefits, subsidies, and

services (where) the expenditure is incurred from or the receipt therefrom forms part of the Consolidated Fund of India;

(c) authentication of the Aadhaar number of an Aadhaar number holder in relation to his demographic and biometric information;

(d) establishment of the Unique Identification Authority of India… to perform functions in pursuance of the objectives above;

(e) maintenance and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;

(f) measures pertaining to security, privacy and confidentiality of information in possession or control of the Authority including information stored in the Central Identities Data Repository; and

(g) offences and penalties for contravention of relevant statutory provisions."

The Preamble to the enactment indicates that Parliament designed the legislation as an instrument of good governance, to secure an "**efficient, transparent and targeted delivery** of subsidies, benefits and services" for which the expenditure is incurred from the Consolidated Fund to resident individuals.

178 The Aadhaar platform is not a social welfare benefit in itself. Essentially, what it seeks to achieve is to provide a unique identity to every resident. This identity, in the form of an Aadhaar number, is obtained upon the submission of demographic and biometric information in the course of enrolment. The legislative design envisages that the identity of the individual is verified through the process of authentication by which the biometric data stored in the central repository is matched with the biometric information submitted for authentication. Aadhaar is a platform for verification of identity

based principally on biometric information. In facilitating the process of establishing the identity of the individual who seeks social welfare benefits envisaged in Section 7, Aadhaar has an instrumental role. It is instrumental in the sense that as a measure of state policy, it seeks to bring about financial inclusion by providing a means of identification to every segment of the population including those who may not have been within the coverage of traditional markers of identity. As an instrument for verifying identity, Aadhaar seeks to ensure that social welfare benefits are obtained by persons eligible to do so and are not captured by the ineligible. Relying on an asserted reliability of biometric markers, the Aadhaar platform attempts to eliminate, or at least to curb rent-seeking behaviour.

The rationale underlying Section 7 is the targeted delivery of services, benefits and subsidies which are funded from the Consolidated Fund of India. In the seven decades since Independence, the Union Government has put into place social welfare measures including the public distribution system, free education, scholarships, mid-day meals and LPG subsidies to ameliorate the conditions of existence of the poor and marginalised. There is a state interest in ensuring that the welfare benefits which the state provides reach those for whom they are intended.

G.3 Identity and Identification

179 Identity is inseparable from the human personality. An identity is a statement of who an individual is. Our identities define who we are. They express what we would wish the world to know us as. The human personality is, at a certain level, all about identity, for it is through the assertion of identity that each individual seeks to preserve the core of his or her humanity. An identity is the persona which an individual puts forth in a multitude of relationships. The significance of our identity lies in our ability to express the core of our beings. When the Constitution protects our right to be and to be what we are, it creates a space where the individual is immune from interference. By recognizing our liberty as autonomous persons, the Constitution recognizes our ability to preserve and shape our identities in interactions with others.

Identity may be, but is not always based upon immutable characteristics that are defined at birth. What is immutable may not be or, at any rate, is not generally understood as being capable of change. But even here, the immutability of our features is relative to our own existence and is capable of being shaped by the social milieu in which human beings lead their lives. Features about our biological being which are defined at birth are, after all, not as constraining upon our identities as is often assumed to be the case. That is because these immutable features are also constantly engaged with our

social and cultural environment. They shape and are influenced by that environment.

180 There is a distinction between identity and identification. Identification is a matter of proof- of establishing that a person is actually, the individual who claims a right or entitlement. In their daily interactions, individuals have to distinguish themselves from others, whether it be in the course of employment, travel, civil union, location, community perspectives, revenue obligations or access to benefits. Identification is a proof of identity or evidence of identity. Identification is mandatory in numerous activities of day to day life: a passport is necessary for international travel, a voter ID is required for exercising electoral rights, a driving license is necessary to ply a vehicle and an arms license is needed to possess a fire arm. The holder of a policy of medical insurance will have a card depicting his or her identity which is a proof of holding a valid policy for availing medical benefits.

181 Under international law, recognition of identity is an obligation of a nation state. Article 6 of the Universal Declaration of Human Rights provides that “everyone has the right to recognition everywhere as a person before the law”. Article 16 of the International Covenant on Civil and Political Rights is in similar terms. Article 8 of the UN Convention on the Rights of the Child mandates that State parties undertake to respect the right of the child to

preserve his or her identity, including nationality, name and family relations as recognized by law without unlawful interference. The importance of identity is recognized by Article 3 of the American Convention on Human Rights. The Inter-American Juridical Committee (IAJC) of the Organisation of American States (OAS) has in fact provided that:

> "12. The right to identity is consubstantial to the attributes and human dignity. Consequently it is an enforceable basic human right *erga omnes* as an expression of a collective interest of the overall international community that does not admit derogation or suspension in cases provided in the American Convention on Human Rights.
>
> …
>
> 15. The Committee considers that the right to identity is, among its most relevant implications and scope, to constitute an autonomous right that is based on the regulations of international law and those that derive from the actual cultural elements considered in the domestic legal systems of the States, in order therefore to satisfy the specificity of the individual, with his or her rights that are unique, singular and identifiable."[306]

182 In **National Legal Services Authority** v **Union of India**[307], this Court held that gender identity is fundamental to and an essential component for the enjoyment of civil rights by the transgender community. Self-determination of identity has been held to be an essential facet of Article 21. In the view of this Court:

> "74. The recognition of one's gender identity lies at the heart of the fundamental right to dignity. Gender, as already indicated, constitutes the core of one's sense of being as well

[306] Opinion on the Right to Identity, 2007, available at http://www.oas.org/en/sla/iajc/docs/ijc_current_agenda_Right_to_Identity.pdf
[307] (2014) 5 SCC 438

> as an integral part of a person's identity. Legal recognition of gender identity is, therefore, part of right to dignity and freedom guaranteed under our Constitution.
> 75. Article 21, as already indicated, guarantees the protection of "personal autonomy" of an individual. In *Anuj Garg* v*. Hotel Association of India*[33] (SCC p. 15, paras 34-35), this Court held that personal autonomy includes both the negative right of not to be subject to interference by others and the positive right of individuals to make decisions about their life, to express themselves and to choose which activities to take part in. Self-determination of gender is an integral part of personal autonomy and self-expression and falls within the realm of personal liberty guaranteed under Article 21 of the Constitution of India."

Identity assumes a complex character in a networked society. Shah adopts the following definition of a networked society[308]:

> "a network society is a society where the key social structures and activities are organized around electronically processed information networks. So it's not just about networks or social networks, because social networks have been very old forms of social organization. It's about social networks which process and manage information and are using micro-electronic based technologies"[309].

183 In a networked society, an individual is a data subject and a quantified self. The individual is a data subject since his or her data is stored in a database. Shah notes that there is an ambivalence about whether the data subject is the individual whose identity becomes the basis of validating the data or whether the data subject is the identity of the individual as it gets constructed through data sets. The individual becomes a quantified self where data which is distributed across various systems is "curated" to form a comprehensive profile of an individual.

[308]Nishant Shah, Identity and Identification – the Individual in the Time of Networked Governance, Socio Legal Review, available at http://www.sociolegalreview.com/wp-content/uploads/2015/12/Identity-and-Identification-the-Individual-in-the-Time-of-Networked-Governance.pdf

[309]Manuel Castells, Conversation with Manuel Castells, Globetrotter, available at http://globetrotter.berkeley.edu/people/Castells/castells-con4.html

184 The Aadhaar project was intended to allow a unique **identity** to enable individuals to "navigate through disconnected and often hostile governmental database systems". Shah notes that ever since 2009, the terms 'identity' and 'identification' were used as part of the Aadhaar project inter-changeably, introducing "a curious conflation and interoperability"[310] between these notions. 'Identification' is the ability of a network device to identify an individual by scanning unique data sets, from personal information to biometric details such as finger print and iris scan, which would be stored in a massive centralized database. UIDAI posited that identification took place through its yes/no mechanism by which the centralised database would provide a response to whether the biometric details submitted for authentication match those in the repository. Technologically, at this level, Aadhaar was to be a **means of identification**. Yet at another level, the Aadhaar project also offered itself as providing a documentary identity to persons who may not have possessed one at all. Shah, in the course of his article, has this to state about the conflation between identity and identification in the Aadhaar project:

> "This ambiguity and conflation cannot merely be attributed to a semantic slip of the keyboard, but to a much larger phenomenon which points to the construction of a new notion of the individual, through big data streams and measures of self-quantification. It offers us a techno-social framework where the machine function of identification is wedded to the human expression of identity, and thus offers an inroad into looking at what happens when our identities are mediated, mitigated, facilitated, and contained by the ways in which the networked technologies of authentication and verification operate. It is a crucial shift where the identity of a person is ontologically defined through the logics and logistics of

[310] Nishant Shah, Identity and Identification – the Individual in the Time of Networked Governance, Socio Legal Review, available at http://www.sociolegalreview.com/wp-content/uploads/2015/12/Identity-and-Identification-the-Individual-in-the-Time-of-Networked-Governance.pdf

> networked computation that form the Aadhaar project. This is why the Aadhaar enrolment system, for instance, does not check the veracity of the information that the individual gives it. For the enrolment, the individual needs no proof to substantiate or validate the information provided. The name, the address, the description, etc. are empty signifiers and it is possible for anybody to assume any identity as long as they give the inviolable data of biometric recognition. Thus, the identity of the person being enrolled and registered is almost insignificant and has value only in how it would now always identify the individual through the credentials or information provided. The Aadhaar network governance system is concerned only with the identifiers rather than the narrative, iterative, forms of identity and expression, and this is where we begin examining the ways in which identity is shaped, understood, and used to construct the notion of an individual in computation systems."[311]

185 Identity includes the right to determine the forms through which identity is expressed and the right not to be identified. That concept is now "flipped" so that identification through identifiers becomes the only form of identity in the time of database governance. This involves a radical transformation in the position of the individual.

The submission which has been urged on behalf of the petitioners is that an individual entitled to the protection of the freedoms and liberties guaranteed by Part III of the Constitution must have the ability to assert a choice of the means of identification for proving identity. Requiring an individual to prove identity on the basis of one mode alone will, it is submitted, violate the right of self-determination and free choice.

[311] Ibid

186 The Aadhaar (Enrolment and Update) Regulations, 2016 stipulate in Regulation 4, the demographic information which is required for enrolment. Regulation 4 is in the following terms:

> "**4. Demographic information required for enrolment**.-
>
> (1) The following demographic information shall be collected from all individuals undergoing enrolment (other than children below five years of age):
>
> (i) Name;
> (ii) Date of Birth;
> (iii) Gender;
> (iv) Residential Address.
>
> (2) The following demographic information may also additionally be collected during enrolment, at the option of the individual undergoing enrolment:
>
> (i) Mobile number;
>
> (ii) Email address.
>
> (3) In case of Introducer-based enrolment, the following additional information shall be collected:
>
> (i) Introducer name;
>
> (ii) Introducer's Aadhaar number.
>
> (4) In case of Head of Family based enrolment, the following additional information shall be collected:
>
> (i) Name of Head of Family;
>
> (ii) Relationship;
>
> (iii) Head of Family's Aadhaar number;
>
> (iv) One modality of biometric information of the Head of Family.
>
> (5) The standards of the above demographic information shall be as may be specified by the Authority for this purpose.

> (6) The demographic information shall not include race, religion, caste, tribe, ethnicity, language, record of entitlement, income or medical history of the resident."

Regulation 9 postulates that at the time of enrolment, the enrolling agency shall inform the individual who is undergoing enrolment of (i) the manner in which the information shall be used; (ii) the nature of recipients with whom the information is intended to be shared during authentication; and (iii) the existence of a right to access information. Under Regulation 10, a resident seeking enrolment has to submit an application for enrolment together with copies of supporting documents for proof of identity, address and date of birth. Schedule II indicates a list of supporting documents which are accepted for verification of identity, address and date of birth. If a resident does not possess the supporting documents, enrolment is contemplated through an introducer or a Head of Family. Schedule II contains as many as eighteen documents which are accepted towards proof of identity and thirty three documents as proof of address. The Aadhaar Act, it has been contended, allows the resident to identify herself through any of the stipulated documents for the purpose of availing an Aadhaar number. The Aadhaar number can be availed of to secure a subsidy, benefit or service under Section 7, the expenditure of which is drawn from the Consolidated Fund of India.

Article 266 of the Constitution provides as follows:

> "266. Consolidated Funds and public accounts of India and of the States

> (1) Subject to the provisions of Article 267 and to the provisions of this Chapter with respect to the assignment of the whole or part of the net proceeds of certain taxes and duties to States, all revenues received by the Government of India, all loans raised by that Government by the issue of treasury bills, loans or ways and means advances and all moneys received by that Government in repayment of loans shall form one consolidated fund to be entitled the "Consolidated Fund of India", and all revenues received by the Government of a State, all loans raised by that Government by the issue of treasury bills, loans or ways and means advances and all moneys received by that Government in repayment of loans shall form one consolidated fund to be entitled "the Consolidated Fund of the State".
> (2) All other public moneys received by or on behalf of the Government of India or the Government of a State shall be credited to the public account of India or the public account of the State, as the case may be
> (3) No moneys out of the Consolidated Fund of India or the Consolidated Fund of a State shall be appropriated except in accordance with law and for the purposes and in the manner provided in this Constitution."

187 The Union Government is the custodian of the Consolidated Fund under Article 266. All revenues received by the government form part of the Consolidated Fund. No part of its proceeds can be "appropriated except in accordance with law and for the purpose and in the manner" which is provided by the Constitution. As the custodian of the fund, the Union Government, it has been submitted by the respondents, had the Aadhaar Act enacted through Parliament. The Act places a restriction on the right of the individual to utilize any other identification save and except for the Aadhaar number, for the purpose of availing of a subsidy, benefit or service that involves an expenditure from the Consolidated Fund. The purpose of making an Aadhaar number mandatory for the delivery of benefits, services and subsidies funded from the Consolidated Fund is to confirm the identity of the individual to whom

the benefit is being transferred. This was in order to ensure that the benefits under social welfare programmes funded by the Consolidated Fund reach the hands of targeted beneficiaries. The Union Government which expends huge sums of money in its welfare schemes was apprised of the fact that money which was meant for the beneficiaries was being siphoned off through ghosts and duplicates. As a result, genuine beneficiaries would be deprived of their basic rights. Cornering of benefits by the creation of bogus identities seriously impacted upon social welfare measures adopted by the Union Government as an instrument of fostering social and economic development. It was to deal with this evil that the Aadhaar project assumed a statutory character in 2016. Through the provisions of the law, Parliament intended that Aadhaar should become an effective instrument of de-duplication. This is premised on the view of the legislating body that the use of biometrics would render it difficult, if not impossible, to obtain fake identities. Aadhaar, in other words, was adopted as a matter of legislative policy to curb the evil of shell companies and ghost identities. Where the State expends large sums on social welfare projects, it has a legitimate interest in ensuring that the resources which it deploys reach the hands of those for whom they are meant.

Thus, there are two important facets of the Aadhaar regime which must be noticed. The first is that under Section 3, it is a voluntary option of the individual to choose Aadhaar as a form of identification. However, if the individual seeks a subsidy, benefit or service for which the expenditure is

incurred from the Consolidated Fund of India, Aadhaar becomes a mandatory requirement. The second important feature is the requirement of informed consent when the individual parts with identity information. The mandate of Section 7 must be understood from the perspective of the obligation imposed on the State to ensure effective and efficient utilization of public resources. Article 266 reinforces that mandate in its stipulation that all monies out of the Consolidated Fund of India can only be appropriated in accordance with law, for the purpose of and in the manner provided by the Constitution. The State is a trustee of public resources. The adoption of Aadhaar is in fulfilment of the doctrine of public trust. The state is under a bounden obligation to ensure that its revenues which are placed in the Consolidated Fund are appropriated in accordance with law and are not diverted for extraneous purposes. These principles have been elucidated in the decisions of this Court in **Natural Resources Allocation, In Re, Special Reference No.1 of 2012**[312], **Centre for Public Interest Litigation** v **Union of India**[313], **Reliance Telecom Limited** v **Union of India**[314].

The mandate of Section 7 is founded on a legitimate state interest. The state has a vital interest in ensuring that public revenues are duly accounted, that the Consolidated Fund is utilized for purposes authorized by law; that funds for development reach genuine beneficiaries and that scarce public resources

[312] (2012) 10 SCC 1
[313] (2012) 3 SCC 1
[314] (2017) 4 SCC 269

meant for those at the foot of the socio-economic ladder are not mis-utilized by rent-seeking behavior.

H Proportionality

188 The petitioners have challenged the constitutional validity of the Aadhaar project and the Aadhaar Act on various grounds including the violation of the fundamental rights of citizens including the right to privacy and dignity. The respondents, in defense, have argued that Aadhaar is an enabler of identity and empowers citizens to realise various facets of the right to life, such as the right to food and livelihood.

189 The learned Attorney General has argued that the use and authentication of the Aadhaar number is a necessary and proportionate measure to ensure targeted delivery of financial benefits and services and to prevent ‘leakages’. He submits that the Aadhaar scheme satisfies the test of proportionality: it has a rational nexus with the goal that it seeks to achieve, and since welfare benefits enhance the right to live with dignity, the latter will prevail over the right to privacy. Mr Rakesh Dwivedi, learned Senior Counsel has argued that the “least intrusive test” is not accepted in Indian jurisprudence. He submits that even if the test were to be accepted, the exercise of determining whether a measure is the least intrusive is a technical issue for which the Court lacks the requisite expertise. He states that this

exercise “cannot be undertaken in the courts with the assistance of lawyers who equally have no expertise in the field” and that “such an exercise involves research, study by the experts and courts cannot substitute the same”. Mr Gopal Sankaranarayanan, learned Counsel, submits that the means adopted “at the moment” are no more than is necessary for ensuring that the “avowed objects” are served, and that they balance individual interests (fundamental rights) with societal interests (directive principles). He further submits that the fact there are various limitations in place ensure that “some balance” is achieved between the breach of privacy and the object sought to be achieved.

This Court must now perform the delicate task of ‘balancing’ these competing interests by subjecting the Aadhaar Act to the proportionality test.

H.I Harmonising conflicting rights

190 In the 2003 edition of his celebrated work, Granville Austin recounts the words of Prime Minister Morarji Desai that freedom and bread are not incompatible, but further adds, ‘Neither could they easily be sought together’.[315] As mentioned earlier, Granville Austin had insightfully spoken about how the strands of the Constitution of unity-integrity, democracy and social revolution could come in conflict with one another creating challenges for those who work with the Constitution.[316] Some of the questions inherent in

[315] Granville Austin, Working a Democratic Constitution: A History of the Indian Experience, Oxford University Press (2003), at page 652
[316] Ibid, at page 651

the Constitution according to him are “Democracy for whom? Justice for whom? What *is* Justice? What are the appropriate means of employing the Constitution’s means’ among citizens, between them and their government?”[317] It was due to the foresight of the framers of the Constitution that they insisted that neither the strand of social revolution nor the strand of democracy was to be pursued at the expense of the other.[318]

The ostensible conflict between bread and freedom has also been explored in the works of Professor Upendra Baxi. In a seminal essay on human rights in 1984 which he calls the “the great gift of classical and contemporary human thought to culture and civilization”[319], he discusses the widening sphere of human rights thought and action to new arenas and constituencies as “New rights arise from the womb of the old.”[320] He draws on the distinction between basic human needs and human rights and argues that the constant struggle between these two forces is the essence of the difference between the right to be human approach and the human rights approach.[321] It is rightly pointed out that a discussion on human rights will always constitute an inherent aspect of the larger debate of development. He opines that whatever meaning maybe ascribed to the term “development”, it must ensure that people will not be deprived of the right to remain human:

[317] Ibid
[318] Ibid
[319] Upendra Baxi, From Human Rights to the Right to be Human: Some Heresies, India International Centre Quarterly, Vol. 13, No. 3/4, Pg.185, (December 1986)
[320] Ibid, at page 185
[321] Ibid

> "Whatever it may be made to mean, "development" must at least mean this: people will be given the right to be and remain human. Total and continuing destitution and impoverishment exposes people to a loss of their humanity. In no society that takes human rights seriously should there be allowed a state of affairs where human beings become sub-human—that is, when they perforce have to surrender even those sonorously recited "inalienable" rights of man… The expression "human rights" presupposes a level at which biological entities are bestowed with the dignity of being called human. The bearers of human rights must have an implicit right to be and remain human, allowing them some autonomy of choice in planning survival."[322]

Thus, the broader matrix of human rights includes within it the inalienable and fundamental right to always 'be and remain human'. Professor Upendra Baxi notes that this broader debate between human rights and the 'right to be human' is reflective of the bread vs freedom conflict. It is noted that historically, freedom might have been chosen over bread due to the vast enumeration of liberal rights it includes, despite the acute awareness that without bread, freedom of speech and assembly, of association, of conscience and religion, of political participation, symbolic adult suffrage may all be meaningless.[323] At the same time, Baxi points out the danger in choosing bread at the cost of freedom, given that historically in the absence of freedom, human beings have been subject to the most egregious indignities:

> "The provision of "bread" may justify indefinite postponement of the provision of any kind of "freedom". In the absence of such freedom, even the promised "bread" may not be realized by the masses; indeed, they even lose, in the process, their power to protest at the indignity of regime sponsored starvation. This, indeed, is a possibility which has materialized more often than not."[324]

[322] Ibid, at page 187
[323] Ibid, at page 186
[324] Ibid, at page 190

Baxi concludes that the choice between bread and freedom is a false antithesis. The challenge is not a choice in the abstract between bread and freedom but rather the balancing of the two:[325]

> "But the issues are not really "bread" and/or "freedom" in the abstract, but rather who has how much of each, for how long, at what cost to others, and why. Some people have both "bread" and "freedom"; others have "freedom" but little "bread" or none at all; yet others have half a loaf (which is better than none, surely!) with or without freedom; and still others have a precarious mix where "bread" is assured if certain (not all) freedoms are bartered."[326]

It is the foremost duty of the State to work towards achieving and maintaining a fine balance, taking into account these myriad considerations. The State must always be guided by the knowledge and sense of duty that in a true democracy, the citizens cannot be made to choose between rights and needs, as they are equally entitled to both. As the sentinel of justice and protector of fundamental rights, it is the responsibility of this Court to act as a check and ensure that government action or inaction does not endanger or threaten to disturb the balance that the Constitution seeks to achieve. It is imperative to remember that both 'bread' and 'freedom' play a vital role in the guaranteeing to our citizens the gamut of human rights and freedoms that make human existence meaningful.

191 While exercising judicial review, courts are often confronted with situations involving conflicts between rights, tensions between individuals arising from the assertion of rights and discord arising out of the assertion of

[325] Ibid, at page 186
[326] Ibid, at page 186

the same right by two or more individuals. Conflicts between rights arise when the assertion of a fundamental human right by an individual impacts upon the exercise of distinct freedoms by others. The freedom of one individual to speak and to express may affect the dignity of another. A person may be aggrieved when the free exercise of the right to speak by someone impinges upon his or her reputation, which is integral to the right to life under Article 21. A conflict will, in such a situation, arise between a right which is asserted under Article 19(1)(a) by one citizen and the sense of injury of another who claims protection of the right to dignity under Article 21. Conflicts also arise when the exercise of rights is perceived to impact upon the collective identity of another group of persons. Conflicts may arise when an activity or conduct of an individual, in pursuit of a freedom recognised by the Constitution, impinges upon the protection afforded to another individual under the rubric of the same human right. Such a situation involves a conflict arising from a freedom which is relatable to the same constitutional guarantee. Privacy is an assertion of the right to life under Article 21. The right to a dignified existence is also protected by the same Article. A conflict within Article 21 may involve a situation when two freedoms are asserted as political rights. A conflict may also envisage a situation where an assertion of a political right under the umbrella of the right to life stands in conflict with the assertion of an economic right which is also comprehended by the protection of life under the Constitution.

Such conflicts require the court to embark on a process of judicial interpretation. The task is to achieve a sense of balance. An ideal situation would be one which would preserve the core of the right for both sets of citizens whose entitlements to freedom appear to be in conflict. Realistically, drawing balances is not a simple task. Balances involve sacrifices and the foregoing of entitlements. In making those decisions, a certain degree of value judgment is inevitable. The balance which the court draws may be open to criticism in regard to its value judgment on the relative importance ascribed to the conflicting rights in judicial decision making. In making those fine balances, the court can pursue an objective formulation by relying upon those values which the Constitution puts forth as part of its endeavour for a just society. Our Constitution has in Part III recognised the importance of political freedom. In Part IV, the Constitution has recognised our social histories of discrimination and prejudice which have led to poverty, deprivation and the absence of a dignified existence to major segments of society. Holding Part III in balance with Part IV is integral to the vision of social and economic justice which the Constitution has sought to achieve consistent with political democracy. Difficult as this area is, a balancing of rights is inevitable, when rights asserted by individuals are in conflict.

192 Several decisions of this Court over the last two decades have sought to bring order to the clash between fundamental rights. In **People's Union for**

Civil Liberties (PUCL) v **Union of India**[327], this Court was called upon to balance the right to information of voters (requiring the disclosure of the assets of candidates and their spouses at an election) with the right to privacy implicit in Article 21. In drawing the balance, a bench of three Judges of this Court gave primacy to the entitlement of citizens to be informed about the affairs of those who would represent them in electoral democracy. As the Court held:

> "121…By calling upon the contesting candidate to disclose the assets and liabilities of his/her spouse, the fundamental right to information of a voter/citizen is thereby promoted. When there is a competition between the right to privacy of an individual and the right to information of the citizens, the former right has to be subordinated to the latter right as it serves the larger public interest. The right to know about the candidate who intends to become a public figure and a representative of the people would not be effective and real if only truncated information of the assets and liabilities is given."[328]

The Court held that the provision contained in the Representation of People Act 1951 for a disclosure of assets and liabilities only to the Speaker or to the Chairman of the House did not adequately protect the citizen's right to information, resulting in a violation of the guarantee of free speech and expression.

193 In **Thalappalam Service Cooperative Bank Limited** v **State of Kerala**[329], this Court dealt with a conflict between the right to information

[327] (2003) 4 SCC 399
[328] Ibid, at page 472
[329] (2013) 16 SCC 82

[(protected by Article 19(1)(a)] and the right to privacy (protected by Article 21). The Court observed:

> "61. The right to information and right to privacy are, therefore, not absolute rights, both the rights, one of which falls under Article 19(1)(a) and the other under Article 21 of the Constitution of India, can obviously be regulated, restricted and curtailed in the larger public interest. Absolute or uncontrolled individual rights do not and cannot exist in any modern State. Citizens' right to get information is statutorily recognised by the RTI Act, but at the same time limitations are also provided in the Act itself, which is discernible from the Preamble and other provisions of the Act."[330]

The Court held that the balance between the right to information and the right to privacy is drawn under the Right to Information Act 2005: if the information which is sought is personal and has no relationship with a public activity or interest, a public authority is not legally bound to provide such information. If the information which is sought is to be made available in the larger public interest, reasons have to be recorded because the person from whom the information is sought has a right to privacy guaranteed by Article 21. **Thalappalam** considered a conflict arising between two fundamental rights, the right to information protected by Article 19(1)(a) and the right to privacy which is protected by Article 21.

194 More recently, in **G Sundarrajan** v **Union of India**[331], a two judge Bench considered a challenge to the establishment of a nuclear power plant on the ground that it would violate the right to life guaranteed by Article 21. Noting that there was a need to draw a balance between the assertion of

[330] Ibid, at page 112
[331] (2013) 6 SCC 620

several rights including the protection of the environment, the Court observed that the larger public interest must prevail:

> "198. We have to resolve the issue whether the establishment of NPP would have the effect of violating the right to life guaranteed under Article 21 to the persons who are residing in and around Kudankulam or by establishing the NPP, it will uphold the right to life in a larger sense. While balancing the benefit of establishing KKNPP Units 1 to 6, with right to life and property and the protection of environment including marine life, we have to strike a balance, since the production of nuclear energy is of extreme importance for the economic growth of our country, alleviate poverty, generate employment, etc. While setting up a project of this nature, we have to have an overall view of larger public interest rather than smaller violation of right to life guaranteed under Article 21 of the Constitution."[332]

In **Subramanian Swamy** v **Union of India**[333], the learned Chief Justice, speaking for a Bench of two judges emphasised the need for a sense of balance when the assertion of fundamental rights by two citizens is in conflict:

> "137…One fundamental right of a person may have to coexist in harmony with the exercise of another fundamental right by others and also with reasonable and valid exercise of power by the State in the light of the directive principles in the interests of social welfare as a whole. The Court's duty is to strike a balance between competing claims of different interests."[334]

Noting that the "balancing of fundamental rights is a constitutional necessity", the Court has attempted to harmonise reputation as an intrinsic element of the right to life under Article 21 with criminal defamation as a restriction under Article 19(2).

[332] Ibid, at page 714
[333] (2016) 7 SCC 221
[334] Ibid, at page 319

195 In **Asha Ranjan** v **Chandrakeshwar Prasad**[335], this Court dealt with a case involving a conflict between the fundamental rights of two individuals within Article 21. There was on the one hand an assertion of the right to life on the part of an individual accused of an offence, who claimed a right to a fair trial, and the protection of the interests of the victim which was also relatable to the same fundamental right under Article 21. In resolving the conflict, the Court gave expression to the need to preserve "paramount collective interests":

> "61…circumstances may emerge that may necessitate for balancing between intra-fundamental rights. It has been distinctly understood that the test that has to be applied while balancing the two fundamental rights or inter fundamental rights, … may be different than the principle to be applied in intra-conflict between the same fundamental right. To elaborate, as in this case, the accused has a fundamental right to have a fair trial under Article 21 of the Constitution. Similarly, the victims who are directly affected and also form a part of the constituent of the collective, have a fundamental right for a fair trial. Thus, there can be two individuals both having legitimacy to claim or assert the right. The factum of legitimacy is a primary consideration. It has to be remembered that no fundamental right is absolute and it can have limitations in certain circumstances. Thus, permissible limitations are imposed by the State. The said limitations are to be within the bounds of law. However, when there is intra-conflict of the right conferred under the same article, like fair trial in this case, the test that is required to be applied, we are disposed to think, it would be "paramount collective interest" or "sustenance of public confidence in the justice dispensation system".[336]

196 These decisions indicate that the process of resolving conflicts arising out of the assertion of different fundamental rights and conflicts within the same fundamental right, necessarily involves judicial balancing. In finding a

[335] (2017) 4 SCC 397
[336] Ibid, at page 433

just balance this Court has applied norms such as the 'paramount public interest'. In seeking to draw the balance between political freedoms and economic freedoms, the Court must preserve the euphony between fundamental rights and directive principles. It is on their co-existence that the edifice of the Constitution is founded. Neither can exist without the other. Democracy rejects the totalitarian option of recognising economic entitlements without political liberty. Economic rights have become justiciable because of the constitutional guarantees founded on freedom and the rule of law. The Constitution is founded on democratic governance and is based on the protection of individual freedom. Freedom comprehends both fundamental political freedoms as well as basic human rights. A just balance between the two is integral to the fulfilment of India's constitutional commitment to realise human liberty in a social context which is cognizant of the histories of discrimination and prejudice suffered by large segments of our society. Where the question is related to the limiting the right to privacy, **Puttaswamy** requires the test of proportionality. It has, therefore, to be tested whether the Aadhaar scheme fulfils the test of proportionality.

197 The test of proportionality, which began as an unwritten set of general principles of law, today constitutes the dominant "best practice" judicial standard for resolving disputes that involve either a conflict between two rights claims or between a right and a legitimate government interest.[337] It has

[337]Jud Mathews and Alec Stone Sweet, All things in Proportion? American Rights Review and the Problem of Balancing, Emory Law Journal, Vol. 60 (2011)

become a “centrepiece of jurisprudence” across the European continent as well as in common law jurisdictions including the United Kingdom, South Africa and Israel.[338] Proportionality is the “defining doctrinal core of a transnational rights-based constitutionalism”[339]. It has been raised to the rank of a fundamental constitutional principle,[340] and represents a global shift from a culture of authority to a culture of justification.[341] Servin argues that jurisprudence on privacy has evolved from the “right to be let alone”, to now being centered around the principle of proportionality.[342]

198 Subjecting the Aadhaar scheme to the test of proportionality does not mean that the Court is second-guessing the wisdom of the legislature. State action must be subjected to judicial scrutiny to ensure that it passes constitutional muster. The test of proportionality stipulates that the nature and extent of the State’s interference 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 goal it seeks to achieve (in this case, purported plugging of welfare leakage and better targeting).

[338]Alec Stone Sweet & Jud Mathews, Proportionality Balancing and Global Constitutionalism, Columbia Journal of Transnational Law, Vol. 47 (2008)

[339]Jud Mathews and Alec Stone Sweet, All things in Proportion? American Rights Review and the Problem of Balancing, Emory Law Journal, Vol. 60 (2011)

[340] Ibid

[341]Moshe Cohen-Eliya and Iddo Porat, Proportionality and the Culture of Justification, American Journal of Comparative Law Vol. 59 (2011) (cited in); Etienne Mureinik, A Bridge to Where? Introducing the Interim Bill of Rights, South African Journal on Human Rights, Vol. 10 (1994)

[342]Andrew B. Serwin, Privacy 3.0 – The Principle of Proportionality, University of Michigan Journal of Law Reform, Vol. 42 (2009)

Within the framework of constitutional interpretation, proportionality serves as a test to determine the extent to which fundamental rights can be limited in the face of legislative intervention which purports to further social and public interest aims. Aharon Barak, the former Chief Justice of the Supreme Court of Israel has described the importance of the proportionality test as thus:[343]

> "Examination of the test of proportionality (in the narrow sense) returns us to first principles that are the foundation of our constitutional democracy and the human rights … Our democracy is characterized by the fact that it imposes limits on the ability to violate human rights; that it is based on the recognition that surrounding the individual there is a wall protecting his right, which cannot be breached even by majority."

In applying the proportionality test, the Court cannot mechanically defer to the State's assertions. Especially given the intrusive nature of the Aadhaar scheme, such deference to the legislature is inappropriate. The State must discharge its burden by demonstrating that rights-infringing measures were necessary and proportionate to the goal sought to be achieved.

H.2 Proportionality standard in Indian jurisprudence

199 In India, the principle of proportionality has a long jurisprudential history which has been adverted to in a judgment[344] of this Court:

> "On account of a Chapter on Fundamental Rights in Part III of our Constitution right from 1950, Indian Courts did not suffer from the disability similar to the one experienced by English Courts for declaring as unconstitutional legislation on the principle of proportionality or reading them in a manner

[343] Adalah v. The Minister of Interior, HCJ 7052/03, English translation available at http://elyon.court.gov.il/files_eng/03/520/070a47/03070520.a47.pdf
[344] Om Kumar v Union of India, (2001) 2 SCC 386

> consistent with the charter of rights. **Ever since 1950, the principle of 'proportionality' has indeed been applied vigorously to legislative (and administrative action) in India.** While dealing with the validity of legislation infringing fundamental freedoms enumerated in Article 19(1) of the Constitution of India…this court had occasion to consider whether the restrictions imposed by legislation were disproportionate to the situation and were not the least restrictive of the choices." (Emphasis supplied)

The early decisions of this Court may not have used the expression "proportionality". But the manner in which the court explained what would be a permissible restraint on rights indicates the seeds or the core of the proportionality standard. Proportionality has been the core of reasonableness since the 1950s. **Chintaman Rao** v **State of Madhya Pradesh**[345] concerned a State legislation which empowered the government to prohibit people in certain areas from manufacturing *bidis*. The object of the law was to ensure the supply of adequate labour for agricultural purposes in areas where *bidi* manufacturing was an alternative source of employment for persons likely to be engaged in agricultural labour. The Court held that the State need not have prohibited all labourers from engaging in *bidi* manufacturing throughout the year in order to satisfy the objective. Justice Mahajan, on behalf of a Constitution Bench held:

> "6.The phrase "reasonable restriction" connotes that **the limitation imposed** on a person in enjoyment of the right **should not be** arbitrary or **of an excessive nature, beyond what is required in the interests of the public**. The word "reasonable" implies intelligent care and deliberation, that is, the choice of a course which reason dictates. **Legislation which arbitrarily or excessively invades the right cannot be said to contain the quality of reasonableness** and unless it strikes a proper balance between the freedom

[345] 1950 SCR 759

> guaranteed in article 19(1)(g) and the social control permitted by clause (6) of article 19, it must be held to be wanting in that quality." (Emphasis supplied)

200 **State of Madras** v **V G Row**[346] considered whether the action of the Tamil Nadu government in declaring an association unlawful violated Article 19(1)(c) of the Constitution. Chief Justice Patanjali Sastri, speaking for the Constitution Bench, propounded what has come to be regarded as a classic statement of the principle of proportionality in our law:

> "15…the test of reasonableness, wherever prescribed, should be applied to each individual statute impugned, and no abstract standard, or general pattern of reasonableness can be laid down as applicable to all cases. The nature of the right alleged to have been infringed, the underlying purpose of the restrictions imposed, the extent and urgency of the evil sought to be remedied thereby, **the disproportion of the imposition**, the prevailing conditions at the time, should all enter into the judicial verdict..." (Emphasis supplied)

The decision of the Constitution Bench in **State of Bihar** v **Kamla Kant Misra**[347] concerned a challenge to the second part of sub-section (6) of Section 144 of the Code of Criminal Procedure on the ground that it violated sub-clauses (b), (c) and (d) of Clause (1) of Article 19 of the Constitution. Justice K S Hegde, speaking for the majority, observed:

> "15.One of the important tests to find out whether a restriction is reasonable is to see …**whether the restriction is in excess of the requirement** or whether it is imposed in an arbitrary manner".[348] (Emphasis supplied)

[346] 1952 SCR 597
[347] (1969) 3 SCC 337
[348] Ibid, at page 345

201 In **Mohammed Faruk** v **State of Madhya Pradesh**[349] a Constitution Bench of this Court held that in determining the proportionality of a measure restricting an individual's right under Article 19(1)(g) of the Constitution, the factors to be taken into consideration would include whether a less drastic restriction would have served the purpose. As the Court held:

> "10…The Court must in considering the validity of the impugned law imposing a prohibition on the carrying on of a business or profession, attempt an evaluation of its direct and immediate impact upon the fundamental rights of the citizens affected thereby and the larger public interest sought to be ensured in the light of the object sought to be achieved, the necessity to restrict the citizen's freedom, [...],**the possibility of achieving the object by imposing a less drastic restraint , [...] or that a less drastic restriction may ensure the object intended to be achieved."**[350]
> (Emphasis supplied)

In **Bishambhar Dayal Chandra Mohan** v **State of Uttar Pradesh**[351], "reasonable restriction" was held to mean that the limitation imposed on the enjoyment of a right should not be arbitrary or of an excessive nature, beyond what is required in the interests of the public.

202 The decision in **Om Kumar** v **Union of India**[352] concerned the quantum of punishment imposed in departmental disciplinary proceedings. Justice M. Jagannadha Rao, speaking for a two judge Bench, defined proportionality in the following terms:

> "28. By 'proportionality', we mean the question whether, while regulating exercise of fundamental rights, the appropriate or

[349] (1969) 1 SCC 853
[350] Ibid, at page 857
[351] (1982) 1 SCC 39
[352] (2001) 2 SCC 386

> **least restrictive choice of measures** has been made by the legislature or the administrator so as to achieve the object of the legislation or the purpose of the administrative order, as the case may be. Under the principle, the Court will see that the legislature and the administrative authority 'maintain a proper balance between the adverse effects which the legislation or the administrative order may have on the rights, liberties or interests of persons keeping in mind the purpose which they were intended to serve'. The legislature and the administrative authority are however given an area of discretion or a range of choices **but as to whether the choice made infringes the rights excessively or not is for the Court**. That is what is meant by proportionality."[353] (Emphasis supplied)

In **Teri Oat Estates** v **U.T., Chandigarh**[354], this Court adopted a similar interpretation of proportionality.

203 In **Modern Dental College and Research Centre** v **State of Madhya Pradesh**,[355] a Constitution Bench of this Court while dealing with a challenge to the vires of the Madhya Pradesh Niji Vyavasayik Shikshan Sanstha (Pravesh Ka Viniyaman Avam Shulk Ka Nirdharan) Adhiniyam, 2007, held that proportionality is the correct test to apply in the context of Article 19(6). Justice A K Sikri, speaking for the Court, held thus :

> "60…Thus, while examining as to whether the impugned provisions of the statute and Rules amount to reasonable restrictions and are brought out in the interest of the general public, the exercise that is required to be undertaken is the balancing of fundamental right to carry on occupation on the one hand and the restrictions imposed on the other hand. This is what is known as 'Doctrine of Proportionality'. **Jurisprudentially, 'proportionality' can be defined as the set of Rules determining the necessary and sufficient conditions for limitation of a constitutionally protected**

[353] Ibid, at page 399
[354] (2004) 2 SCC 130
[355] (2016) 7 SCC 353

> **right by a law to be constitutionally permissible..."**[356]
> (Emphasis supplied)

While expounding on the theory of proportionality, Justice AK Sikri referred to Aharon Barak's seminal book[357] on proportionality:

> "60…A limitation of a constitutional right will be constitutionally permissible if: (i) it is designated for a proper purpose; (ii) the measures undertaken to effectuate such a limitation are rationally connected to the fulfilment of that purpose; (iii) the measures undertaken are necessary in that there are no alternative measures that may similarly achieve that same purpose with a lesser degree of limitation; and finally (iv) there needs to be a proper relation ('proportionality stricto sensu' or 'balancing') between the importance of achieving the proper purpose and the social importance of preventing the limitation on the constitutional right."[358]

Justice Sikri held that laws limiting constitutional rights must satisfy the test of proportionality:

> "63…The law imposing restrictions will be treated as proportional if it is meant to achieve a proper purpose, and if the measures taken to achieve such a purpose are rationally connected to the purpose, **and such measures are necessary**….[359]
>
> 64. The exercise which, therefore, to be taken is to find out as to **whether the limitation of constitutional rights is for a purpose that is reasonable and necessary in a democratic society and such an exercise involves the weighing up of competitive values, and ultimately an assessment based on proportionality i.e. balancing of different interests."**[360] (Emphasis supplied)

[356] Ibid, at page 412
[357] Aharon Barak, Proportionality: Constitutional Rights and their Limitations, Cambridge University Press (2012)
[358] Ibid, at page 412
[359] Ibid, at page 414
[360] Ibid, at page 415

204 In **KS Puttaswamy** v **Union of India**[361], one of us (Chandrachud J.), speaking for four judges, laid down the tests that would need to be satisfied under our Constitution for violations of privacy to be justified. This included the test of proportionality:

> "325…A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them."[362]

The third principle (iii above) adopts the test of proportionality to ensure a rational nexus between the objects and the means adopted to achieve them. The essential role of the test of proportionality is to enable the court to determine whether a legislative measure is disproportionate in its interference with the fundamental right. In determining this, the court will have regard to whether a less intrusive measure could have been adopted consistent with the object of the law and whether the impact of the encroachment on a fundamental right is disproportionate to the benefit which is likely to ensue. The proportionality standard must be met by the procedural and substantive aspects of the law.

[361] (2017) 10 SCC 1
[362] Ibid, at page 509

Justice Sanjay Kishan Kaul, in his concurring opinion, suggested a four-pronged test as follows[363]:

> "(i)The action must be sanctioned by law;
> (ii) The proposed action must be necessary in a democratic society for a legitimate aim;
> (iii) The extent of such interference must be proportionate to the need for such interference;
> (iv) There must be procedural guarantees against abuse of such interference."

The 'test of proportionality' is a judicially-entrenched principle which has invigorated fundamental rights jurisprudence in the country. The application of the proportionality standard in rights-based adjudication is well-recognised across diverse jurisdictions.

H.3 Comparative jurisprudence

205 Since some of the concerns raised by the Aadhaar scheme have arisen for the first time in India, it would be appropriate to discuss judgments of foreign jurisdictions which have inquired into the proportionality of measures many of them similar to those prescribed under the Aadhaar Act.

206 The Privy Council formulated the parameters of proportionality in **Elloy de Freitas** v **Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing**,[364] elaborating a three-fold test:

> "whether: (i) the legislative objective is sufficiently important to justify limiting a fundamental right; (ii) the measures designed

[363] Ibid, at para 638
[364] [1999] 1 AC 69

> to meet the legislative objective are rationally connected to it; and (iii) the means used to impair the right or freedom are no more than is necessary to accomplish the objective."

Subsequently in **Huang (FC)** v **Secretary of State for the Home Department**,[365] the House of Lords added a fourth parameter which is "the need to balance the interests of society with those of individuals and groups."

207 In the **Federal Census Act Case (Volkszählungsurteil)**,[366] the Federal Constitutional Court of the Federal Republic of Germany dealt with a challenge to the German Federal Census Act, 1983, which provided for collection of citizens' basic personal information, including, *inter alia*, source of income, occupation, supplementary employment, educational background and hours of work. Certain provisions provided for transmission of statistical data to local governments for the purposes of regional planning, surveying, environmental protection, and redrawing of election districts. The Court struck down provisions permitting transfer of statistical data to local authorities on the ground that they enabled authorities to compare census data with local housing registries. The Court observed that the combination of statistical data and a personalized registry could lead to the identification of particular persons, which would lead to a chilling effect upon individuals' right to informational self-determination.

[365] [2007] UKHL 11
[366] (1983) 65 BVerfGE 1

The Court developed a 'fundamental right of informational self-determination' drawing from Articles 1(1) and 2(1) of the German Constitution, which protect the fundamental right to human dignity and the right to freely develop one's personality. Explaining the importance of this right in the context of risks occasioned by modern data processing, the Court noted that:

> "The freedom of individuals to make plans or decisions in reliance on their personal powers of self-determination may be significantly inhibited if they cannot with sufficient certainty determine what information on them is known in certain areas of their social sphere and in some measure appraise the extent of knowledge in the possession of possible interlocutors. A social order in which individuals can no longer ascertain who knows what about them and when and a legal order that makes this possible would not be compatible with the right to informational self-determination…This would not only restrict the possibilities for personal development of those individuals but also be detrimental to the public good since self-determination is an elementary prerequisite for the functioning of a free democratic society predicated on the freedom of action and participation of its members…The fundamental right guarantees in principle the power of individuals to make their own decisions as regards the disclosure and use of their personal data."[367]

The Court, while recognizing the right to informational self-determination, observed that distinct silos of data "can be pieced together with other data collections particularly when individual integrated information systems are built up – to add up to a partial or virtually complete personality profile," and that too with, "the person concerned having no means of controlling its truth and application."[368] Of crucial importance is the Court's observation that the right to informational self-determination is particularly endangered because

[367]Jürgen Bröhmer et al., "BVerfGE 65, 1 - Census Act" in 60 Years German Basic Law: The German Constitution and its Court - Landmark Decisions of the Federal Constitutional Court of Germany in the Area of Fundamental Rights (Suhainah Wahiduddin ed.), (2012) at Pages 147-148, available at http://www.kas.de/wf/doc/kas_32858-1522-1-30.pdf?121123115540

[368] Census Act Case, (1983)

in reaching decisions, one no longer has to rely on manually collected registries and files. Today, the technical means of storing individual statements about personal or factual situations of a certain or verifiable person with the aid of automatic data processing are practically unlimited and can be retrieved in a matter of seconds irrespective of distances.[369]

The Court noted, however, that the right to informational self-determination is not absolute and that public sector entities could collect personal data under certain conditions. The Court held that there must be a statutory basis for this informational activity, and that it must satisfy the principle of proportionality. On the need for a statutory basis, the Court held that:

> "The use of the data is limited to the purpose specified by law. If for no other reason than because of the dangers associated with automated data processing, protection is required against unauthorized use - including protection against such use by other governmental entities - through a prohibition on the transfer and use of such data"[370]
> "Clearly defined conditions must be created for processing to ensure that individuals do not become mere data subjects in the context of the automated collection and processing of the information pertaining to their person. Both the absence of a connection with a specific purpose that can be recognized and verified at all times and the multifunctional use of data, reinforce the tendencies that are to be checked and restricted by data-protection legislation, which represents the concrete manifestation of the constitutionally guaranteed right to informational self-determination."[371]

On the principle of proportionality, the Court held that:

> "The legislature must in its statutory regulations respect the principle of proportionality. This principle, which enjoys constitutional status, follows from the nature of the

[369]Census Act Case, (1983)
[370] Ibid, at page 150.
[371] Ibid, at page 151

> fundamental rights themselves, which, as an expression of the general right of the public to freedom from interference by the state, may be restricted by the public powers in any given case only insofar as indispensable for the protection of public interests … In view of the threats described above that arise from the use of automated data processing, the legislature must more than was the case previously, adopt organizational and procedural precautions that work counter to the threat of violation of the right of personality …"[372]
> "The survey program of the 1983 Census Act also satisfies, to the extent relevant to the matter under review, the principle of proportionality. A measure to achieve the intended purpose must therefore be suitable and necessary; the intensity of the attendant action may not be disproportionate to the importance of the matter and the compromises imposed upon the public."[373]

The Court concluded that according to the principles of purpose specification and proportionality, not only must the purpose for which data is being collected be specified at the time of collection, but the data acquired must also not exceed that which is absolutely necessary for accomplishing the specified purpose. In light of this, the Court directed the German Parliament to amend the law in certain particulars before the census could be carried out, and to close all loopholes in the law that may lead to abuses in the collection, storage, use and transfer of personal data.

208 The ECtHR dealt with whether retention of DNA samples of individuals who were arrested but who were later acquitted or had charges against them dropped was a violation of the right to privacy. In **S and Marper** v **United**

[372] Ibid, at page 149
[373] Ibid, at page 154

Kingdom,[374] the ECtHR noted the "blanket and indiscriminate nature of the power of retention":

> "The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken—and retained—from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances."[375]

The Court concluded that the retention constituted a disproportionate interference with the Applicants' right to privacy:

> "125…That the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. **Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society…**" (Emphasis supplied)

The Court rejected the government's arguments that fingerprints constituted neutral, objective, irrefutable and unintelligible material, holding that they contained unique information about an individual, allowing their precise

[374] (2008) 48 EHRR 1169
[375] Ibid, at Paragraph 119

identification in certain circumstances. The Court concluded that the collection of fingerprints was therefore capable of affecting private life, and retention of such information without consent "cannot be regarded as neutral or insignificant."

209 In 2012, the French Constitutional Council ("Council") – the body that reviews the constitutionality of French laws – declared four provisions of the Identity Protection Act, which proposed the introduction of a new national biometric ID for citizens, to be unconstitutional.[376] Articles 3 and 5 were among the provisions that were struck down. Article 3 authorized that the national ID card may contain data which would enable the holder to identify himself or herself on electronic communication networks or use his or her electronic signature. The Article stated that:

> "If requested by its holder, the national identity card may also contain data, stored separately, enabling it to identify itself on electronic communication networks and to affix its electronic signature. Upon each use, the interested party shall decide which identification data are to be transmitted electronically."

The Council observed that Article 3 did not stipulate the nature of the data that was being collected, nor did it provide any guarantee of maintaining confidentiality. Thus, the Council declared Article 3 to be unconstitutional:

> **"**that the provisions of Article 3 do not specify either the nature of the "data" through which these functions may be implemented or the guarantees ensuring the integrity and confidentiality of this data; that they do not define in any

[376]Decision No. 2012-652 DC of 22 March 2012 by Le Conseil Constitutionnel, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/case-law/sample-of-decisions-in-relevant-areas-dc/decision/decision-no-2012-652-dc-of-22-march-2012.105428.html

> greater detail the conditions under which the persons implementing these functions are to be authenticated, especially when they are minors or are subject to legal protection; that accordingly, Parliament acted in excess of its powers; that accordingly Article 3 must be ruled unconstitutional;"

Article 5 allowed for the establishment of a database of personal information which would include, in addition to the marital status and residence of the holder, their height, eye colour, fingerprints and photograph for the issuance of French passports and national ID cards and for conducting investigations involving certain offences if authorised by a public prosecutor or a judge.

The Council relied on Article 34 of the French Constitution to hold that it was incumbent upon the Parliament to strike a balance between safeguarding public order and bringing offenders to justice on one hand, and the right to privacy on the other. The Council placed reliance on the Declaration of the Rights of Man and the Citizen of 1789. Article 2 of the Declaration states "The aim of every political association is the preservation of the natural and imprescriptible rights of Man. These rights are liberty, property, safety and resistance to oppression". The Council held that the liberty proclaimed by Article 2 includes the right to respect for private life, and accordingly, that "the collection, registration, conservation, consultation and communication of personal data must be justified on grounds of general interest and implemented in an adequate manner, proportionate to this objective." The Council held that Article 5 violated the French Constitution as the nature of the data collected was such that it would facilitate the identification of French

citizens on the basis of their fingerprints, thus breaching the right to respect for private life:

> "Considering however that, given its object, this database containing personal data is intended to collect data relating to almost all of the population of French nationality; that **since the biometric data registered in this file, including in particular fingerprints, are themselves liable to be compared with physical traces left involuntarily by an individual or collected unbeknown to him, they are particularly sensitive; that the technical characteristics of this database as defined by the contested provisions enable it to be consulted for purposes other than the verification of an individual's identity**; that the provisions of the act referred authorise this database to be consulted or viewed not only in relation to the issue or renewal of identity and travel documents or to verify the holder of such a document, but also for other purposes of an administrative nature or by the investigating police;…
> …having regard to the nature of the data registered, the scope of this processing, its technical characteristics and the conditions under which it may be consulted, the provisions of Article 5 violate the right to respect for privacy in a manner which cannot be regarded as proportionate to the goal pursued; that accordingly, Articles 5 and 10 of the act must be ruled unconstitutional…" (Emphasis supplied)

Subsequently, Law 2012-410 of March 27, 2012, on Identity Protection was published in the official gazette of France, without Articles 3 and 5, which had been rendered unconstitutional by the Council.[377]

210 **Aycaguer** v **France**[378] concerned the applicant's refusal to undergo biological testing, the result of which was to be included in the national computerised DNA database. As a result of his refusal, he was convicted. The ECtHR held that the regulations on the storage of DNA profiles did not provide

[377] LOI n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, available at https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582411&dateTexte=&categorieLien=id.
[378] Application no. 8806/12

individuals with sufficient protection, due to its duration and the fact that the data could not be deleted. The Court concluded that the regulations failed to strike a balance between competing public and private interests and held, unanimously, that there had been a violation of Article 8 (right to respect for private life) of the European Convention on Human Rights.

211 The Conseil d'Etat[379] in **Association pour la promotion de l'image**[380] was asked whether a decree regulating the use and storage of data from biometric passports was lawful. One of the stipulations of the decree was that eight fingerprints were stored by the authorities, while only two were required for the passport. The Conseil d'Etat stated that the collection and retention of six more fingerprints to be centrally stored was irrelevant and excessive in relation to the purpose of the computerized database.

212 In **Digital Rights Ireland Ltd** v **Minister**,[381] the Court of Justice of the European Union held that the EU legislature had exceeded the limits of the principle of proportionality in relation to certain provisions of the Charter of Fundamental Rights of the European Union – Articles 7, 8 and 52(1) – by adopting the Data Retention Directive. According to the Directive, member states were obliged to store citizens' telecommunications data for a minimum of 6 months and a maximum of 24 months. The Directive empowered police

[379]The Conseil d'Etat (Council of State) is a body of the French government that acts as legal advisor of the executive branch and as the supreme court for administrative justice
[380] Conseil d' Etat in France, 26 October 2011
[381] C-293/12 and C-594/12

and security agencies to request access to details such as IP address and time of use of all e-mails, phone calls and text messages sent or received.

The Court applied the test of proportionality to the measures. It was noted that metadata allows officials to make precise conclusions about a person's private life, and dragnet data collection creates a chilling effect based on the sense that one's life is subject to surveillance at all times. On the nature of metadata, the Court observed that:

> "Taken as a whole, [metadata] may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[382]

The Court found that surveillance serves an important public interest – public security – and that the right to security is itself a fundamental right under Article 6 of the Charter.[383] However, the Court adopted a two-pronged proportionality test to conclude that the Directive's retention and access requirements were not proportional to that interest.

> "…According to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives."[384]

[382] Ibid, at para 27
[383] Ibid, at para 42
[384] Ibid, at para 46

The retention measure was held to be unnecessary to fulfill the objective of fighting against serious crime:

> "As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques**. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.** (Emphasis supplied)**"**[385]

The Court criticized the Directive for failing to lay down any clear or precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It observed that the Directive was overbroad because it applied to all data, regardless of the existence of suspicion, and contained no criteria for limiting government access or safeguards for preventing abuse:

> "…Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime…
> …Whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."[386]
> "Not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any

[385] Ibid, at para 51
[386] Ibid, at paras 57-59

> objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law."[387]

The Court concluded that the Directive failed to set out "clear and precise rules"[388] for access or for how states should judge the period of time for which data should be held, and "entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[389] The Court struck down the Directive on the basis of the scope of the data to be retained,[390] the lack of limits imposed on state access,[391] and the failure to distinguish between the treatment of data based on its usefulness and relevance.[392]

Of crucial importance is the Court's emphasis that the judicial review of the EU legislature's discretion "should be strict" because of "the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with

[387] Ibid, at para 60
[388] Ibid, at para 54
[389] Ibid, at para 65
[390] Ibid, at paras 56 –58
[391] Ibid, at paras 60-62
[392] Ibid, at paras 59, 63– 64

that right caused by Directive 2006/24".[393] In addition, the Court emphasized that even highly important objectives such as the fight against serious crime and terrorism cannot justify measures which lead to forms of interference that go beyond what is 'strictly necessary'.[394]

213 In **Michael Schwarz** v **Stadt Bochum**,[395] the Court of Justice of the European Union was called upon to examine the validity of a provision in a Council Regulation that obliged persons applying for a passport to provide fingerprints which would be stored in that passport. In considering whether this regulation was valid and necessary, the Court observed:

> "…Article 1(2) of Regulation No 2252/2004 does not provide for **the storage of fingerprints except within the passport itself, which belongs to the holder alone.[396]**
> **The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself…be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the European Union.[397]**
> In those circumstances, the arguments put forward by the referring court concerning the risks linked to possible centralisation cannot, in any event, affect the validity of that regulation and would have, **should the case arise, to be examined in the course of an action brought before the competent courts against legislation providing for a centralised fingerprint base.** In the light of the foregoing, it must be held that Article 1(2) of Regulation No 2252/2004 does not imply any processing of fingerprints that would go beyond what is necessary in order to achieve the aim of protecting against the fraudulent use of passports. It follows that the interference arising from Article 1(2) of Regulation No 2252/2004 is justified by its aim of protecting against the fraudulent use of passports."[398]

[393] Ibid, at para 48
[394] Ibid, at para 51
[395] [2013] EUECJ C-291/12
[396] Ibid, at para 60
[397] Ibid, at para 61
[398] Ibid, at para 62

The Court held that although the taking and storing of fingerprints in passports constituted an infringement of the right to respect for private life and the right to protection of personal data, Article 1(2) of Regulation No 2252/2004 did not imply any processing of fingerprints that would go beyond what is necessary in order to achieve the aim of protecting against the fraudulent use of passports and was therefore valid.

214 In **Madhewoo** v **The State of Mauritius**,[399] the Judicial Committee of the Privy Council heard an appeal from a judgment of the Supreme Court of Mauritius regarding the constitutionality of the provisions of The National Identity Card (Miscellaneous Provisions) Act, 2013. The Act required biometric information including fingerprints, to be stored in a central register in which particulars of the identity of every citizen of Mauritius were to be recorded.

The Supreme Court upheld provisions of the Act that provided for the compulsory taking of fingerprints. However, the Court struck down those provisions that provided for the biometric data to be stored in a central register. The Appellant appealed to the Committee, contending that the provisions providing for the compulsory taking of fingerprints should also be struck down as unconstitutional.

The appellant challenged the following provisions of the Act: (i) the storage of data in a register in electronic data under Section 3; (ii) the obligation to

[399] [2016] UKPC 30

provide biometric information under Section 4; (iii) the collection of information, in electronic form, for a national ID card under Section 5; (iv) the compulsory production of an identity card to a policeman under Section 7(1A) in response to a request under Section 7(1)(b); and (v) the gravity of the potential penalties for non-compliance under Section 9(3), before the Mauritian Supreme Court. The challenge was on the ground that the implementation of the biometric identity card and the permanent storage of biometric data contravened provisions of the Mauritian Constitution and the Civil Code.

Regarding the challenge to Section 4 (2)(c) of the Act, which provided that, "every person who applies for an identity card shall allow his fingerprints, and other biometric information about himself, to be taken and recorded … for the purpose of the identity card," the Supreme Court noted that the right to privacy under Section 9(1) of the Constitution was not an absolute right and interference with that right could be permitted under Section 9(2), if a law that interfered with that right was in the interest, *inter alia*, of public order. The Committee noted the Supreme Court's approach to determining whether Section 4(2)(c) fell foul of the Constitution, which was based on the test laid down in **S and Marper** v **The United Kingdom**[400]:

> "In addressing the question whether section 4(2)(c) of the 1985 Act (as amended) was reasonably justifiable in a democratic society the Supreme Court drew on jurisprudence of the European Court of Human Rights in S v The United Kingdom…In substance the Court asked whether the

[400] [2008] ECHR 1581

> measure pursued a legitimate aim, whether the reasons given by the national authorities for the interference in pursuit of that aim were relevant and sufficient, and whether the measure was proportionate to the aim pursued. This evaluation is essentially the same as that adopted by the courts in the United Kingdom in relation to article 8(2) of the ECHR, in which the courts ask themselves (a) whether the measure is in accordance with the law, (ii) whether it pursues a legitimate aim, and (iii) whether the measure will give rise to interferences with fundamental rights which are disproportionate, having regard to the legitimate aim pursued. In relation to (iii), the courts ask themselves: (a) whether the objective is sufficiently important to justify a limitation of the protected right, (b) whether the measure is rationally connected to the objective, (c) whether a less intrusive measure could have been used without compromising the achievement of the objective (in other words, whether the limitation on the fundamental right was one which it was reasonable for the legislature to impose), and (d) whether the impact of the infringement of the protected rights is disproportionate to the likely benefit of the measure"

The Committee reproduced the Mauritian Supreme Court's holding that the provisions of the Act which enforced the compulsory taking and recording of fingerprints interfered with the Appellant's rights guaranteed under section 9(1) of the Constitution,[401] but that the law was justifiable on grounds of public interest and public order:

> "We find that it can hardly be disputed that the taking of fingerprints within the applicable legal framework pursues the legitimate purpose of establishing a sound and secure identity protection system for the nation and thus answers a pressing social need affording indispensable protection against identity fraud. Such a purpose, as has been amply demonstrated, is vital for proper law enforcement in Mauritius. Furthermore, taking into consideration the appropriate safeguards in the taking of fingerprints for their insertion in the cards, and the relatively limited degree of interference involved, we are led to conclude that such interference is proportionate to the legitimate aim pursued."[402]

[401] Maharajah Madhewoo v. The State of Mauritius & Anr., 2015 SCJ 177, at page 23
[402] [2016] UKPC 30, at page 10

Thus, the Mauritian Supreme Court upheld provisions of the Act which provided for the compulsory taking of fingerprints. The Appellant also challenged Section 3 of the Act, which provided for biometric data to be stored in a register. The Supreme Court, after taking into consideration witness testimonies on the purpose of data collection, noted that though there may have been a legitimate aim for storing and collecting this data, "sufficiently strong reasons…to establish that such storage and retention of data for an indefinite period is proportionate to the legitimate aim pursued" were not established.[403] Thus, the Court held that:

> "… it is inconceivable that there can be such uncontrolled access to personal data in the absence of the vital safeguards afforded by judicial control. The potential for misuse or abuse of the exercise of the powers granted under the law would be significantly disproportionate to the legitimate aim which the defendants have claimed in order to justify the retention and storage of personal data under the Data Protection Act."[404]

Thus, while the Supreme Court noted that the law providing for the storage and retention of personal biometric data constituted a permissible derogation under Section 9(2) of the Constitution,[405] it held that since the Respondent had not established that provisions dealing with storage and retention were reasonably justifiable in a democratic society, they were unconstitutional.

[403] Ibid, at page 31
[404] Ibid, at page 33
[405] Article 9. Protection of privacy of home and other property: (2) Nothing contained in or done under the authority of any law shall be held to be consistent with or in contravention of this section to the extent that the law in question makes provision - (a) in the interests of defence, public safety, public order, public morality, public health, town and country planning, the development or utilisation of mineral resources or the development or utilisation of any other property in such a manner as to promote the public benefit; (b) for the purpose of protecting the rights or freedoms of other persons; (c) to enable an officer or agent of the government or a local authority, or a body corporate established by law for public purpose, to enter on the premises of any person in order to value those premises for the purpose of any tax, rate or due, or in order to carry out work connected with any property that is lawfully on those premises and that belongs to the government, the local authority or that body corporate, as the case may be; or (d) to authorise, for the purpose of enforcing the judgement or order of a court in any civil proceedings, the search of any person or property by order of a court or the entry upon any premises by such order, Except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society

The Judicial Committee did not interfere with the Supreme Court's decision. However, it noted an inconsistency in the Supreme Court's order wherein it held that the law providing for the storage and retention of fingerprints and other biometric data constitutes a permissible derogation under section 9(2) of the Constitution, whilst simultaneously holding the same provisions to be unconstitutional. The Committee reconciled the holding to be:

> "A law providing for the storage and retention of fingerprints and other personal biometric data regarding the identity of a person **in principle** constitutes a permissible derogation, in the interests of public order, under section 9(2) of the Constitution." (Emphasis supplied)

215 The learned Attorney General has relied on cases from other jurisdictions to buttress his contention that the collection and use of biometric information for various services have been found to be legal. 'Biometric data[406]' is defined in the General Data Protection Regulation thus:

> "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."

The learned Attorney General cited the following judgments of the US Supreme Court: **Vernonia School District 47J** v **Acton** ("**Acton**"),[407] **Skinner** v **Railway Labor Executives' Association** ("**Skinner**"),[408] **Whalen** v **Roe** ("**Whalen**"),[409] **United States** v **Dionisio** ("**Dionisio**")[410] and **Bowen** v **Roy**

[406] Article 4(14)
[407] 515 U.S. 646 (1995)
[408] 489 U.S. 602 (1989)
[409] 429 U.S. 589 (1977)
[410] 410 U.S. 1 (1973)

("**Bowen**").[411] Only **Acton**, **Skinner** and **Dionisio** were decided in the context of biometrics, which as we have found before, forms the bedrock of the Aadhaar program. In **Acton**, the court held that the action of the authorities conducting random drug testing of high school athletes was legal since the conditions of collection were nearly identical to those typically encountered in public restrooms. As a result, it was found that, privacy interests of the students were negligibly affected. In **Skinner**, the court found the actions of the Federal Railroad Administration ("**FRA**") requiring mandatory blood and urine testing of employees involved in train accidents to be constitutional. The court observed that railroad accidents, if not prevented, could cause massive loss of life and property. Further, it was held that FRA's regulations fulfilled a "special need" because of the interest of the government in ensuring safety of railroads and were therefore, not "an undue infringement on the justifiable expectations of privacy of covered employees". In **Whalen**, the Court found that retention of patients' information such as their name, address and age, under the New York State Controlled Substances Act, 1972, was not in violation of the constitutional right to privacy as the Court was satisfied that the statute provided for proper safeguards and redressal against theft and loss of information. In **Dionisio**, the Court found no constitutional infirmity with the issuance of a subpoena to procure voice recording exhibits by tapping telephones in order to investigate crimes. The Court held that "neither the summons to appear before the grand jury, nor its directive to make a voice recording, infringed upon any interest protected by the Fourth Amendment".

[411] 476 U.S. 693 (1986)

The Court observed that a compelled display of identifiable physical characteristics does not infringe upon an "interest protected by the privilege against compulsory self-incrimination". In **Bowen**, the Court upheld the provisions of a welfare scheme which required citizens to furnish their social security number, rejecting the argument that the use of a social security number violated the Appellant's Native American beliefs. The Court held that the Free Exercise Clause of the First Amendment could not be construed to place a requirement on the government to conduct its internal affairs in consonance with the religious beliefs of particular citizens.

In **In re Crawford**,[412] the Ninth Circuit upheld provisions of the Bankruptcy Code which mandated public disclosure of a Bankruptcy Petition Preparers' Social Security Number on documents submitted to the Court, noting that the provision had been enacted to serve governmental interests of preventing fraud and providing public access to judicial proceedings.

216 Some decisions of lower courts in the US which have considered the validity of laws or actions of the State deploying biometrics and which have been cited by the respondents are: **Haskell** v **Harris** ("**Haskell**"),[413] **Utility Workers Union of America** v **Nuclear Regulatory Commission** ("**UWUA**"),[414] **Nicholas A Iacobucci** v **City of Newport** ("**Iacobucci**"),[415]

[412] 194 F.3d 954 (9th Cir. 1999)
[413] 669 F.3d 1049 (9th Cir. 2012)
[414] 664 F. Supp. 136 (S.D.N.Y. 1987)
[415] 785 F.2d 1354 (6th Cir. 1986)

Thom v **New York Stock Exchange** (“**Thom**”),[416] **Perkey** v **Department of Motor Vehicles** (“**Perkey**”),[417] **Buchanan** v **Wing** (**Buchanan**),[418] **People** v **Stuller** (“**Stuller**”),[419] **United States** v **Kelly** (“**Kelly**”)[420] and **Brown** v **Brannon** (“**Brannon**”).[421] At first blush, it does seem that these cases support the Respondents’ stand, however, we cannot lose sight of the context in which the courts came to the conclusion emphasised by the respondents in support of their submissions. In **Haskell**, the Ninth Circuit found a Californian law which authorized law enforcement officers to collect DNA in the form of a sample from the buccal swab of the mouth of felony arrestees, who had not been convicted, to be constitutional. The Court noted that the arrestees had reduced privacy interests; the physical intrusion of collecting a buccal swab was *de minimis* in nature; there were stringent limits on the manner in which the information was to be used; and the interest of the State in deterring future criminal acts to exculpate innocent arrestees aided in prison administration and law enforcement. For the above reasons, the Court found that the infringement of privacy of the felony arrestees was justified. In **UWUA**, the Ninth Circuit ruled that a law requiring individuals working in nuclear power facilities to submit their fingerprints for identification and criminal history record checks was not unconstitutional. In **Iacobucci**, an ordinance which required employees of liquor selling establishments which permitted nude dancing, to be fingerprinted and photographed by the police department, was held

[416] 306 F. Supp. 1002 (S.D.N.Y. 1969)
[417] (1986) 42 Cal. 3d 185
[418] N.Y.S.2d 865
[419] 10 Cal. App.3d 582 (1970)
[420] 55 F.2d 67 (2d Cir. 1932)
[421] 399 F. Supp. 133 (M.D.N.C. 1975)

constitutional. The Court observed that fingerprinting and photographing of employees of retail liquor establishments bore a rational relationship to the legitimate aim of elimination of crime. In **Thom**, a New York statute, which as a condition of employment, required all the employees of member firms of national stock exchanges to be fingerprinted, was upheld. The Court ruled that fingerprinting was a necessary means of verifying the existence or non-existence of a prior criminal record, in order to avert any threat posed by an employee who was in a position to commit theft of securities. In **Perkey**, the Californian Supreme Court upheld the actions of the state mandating an individual to provide a fingerprint in order to obtain a driver's license. The Court held that fingerprint technology was the only reliable means of ensuring the integrity of the records of the department of motor vehicles as other methods such as handwriting specimens and photographs were not reliable. Thus, the submission of fingerprints as part of the license application process, bore a rational relationship to the State's goal of promoting safe and lawful use of highways. In **Buchanan**, the Court upheld the eligibility requirement for a welfare aid scheme which mandated participation in an identity verification procedure known as Automated Finger Imaging System (AFIS), rejecting the challenge based on religious beliefs of the Petitioner. The Court held that the Petitioner had failed to prove that the AFIS involved any invasive procedures, noting that she had acknowledged that she had never seen finger imaging performed and had no idea whether a laser was involved. In **Stuller**, the constitutionality of a law which required "temporary and itinerant classes of

employees" to undergo fingerprinting in order to protect "visitors and residents" of a resort city from crime and loss, both against people and against property, was upheld. In **Kelly**, the Circuit Court of Appeals rejected a claim for return of fingerprints of the defendant which had been obtained after he had been arrested by prohibition agents, holding that there was no reason to interfere with a method of identifying persons "charged with a crime". In **Brannon**, the court held that a law requiring "massagists" to submit their fingerprints, photographs and reports of their medical examinations in order to obtain licenses was valid, noting that the fingerprints and photographs would aid in their identification as well as in the enforcement of criminal statutes relating to public morality and decency.

217 The cases cited by the learned Attorney General would not be applicable in the context of the Aadhaar program. The cases cited dealt with narrowly tailored legislations set out to achieve very specific objectives. For instance, courts upheld statutes aimed at protecting a nuclear facility or to prevent theft of securities, where incidents of sabotage or breach of security would have led to national disasters. These national disasters in turn would have resulted in the immediate loss of human life or in a situation of financial emergency. Such laws, were therefore, enacted in order to assuage security concerns which, if not implemented, could lead to incidents of massive losses of life and property.

Some of the statutes upheld, permitted collection of DNA samples, fingerprints and photographs for identification. The objective behind these laws was prevention of crime, albeit on a comparatively smaller scale. Moreover, the courts in these cases were also satisfied that the procedures involved in collecting biometrics were not invasive enough to strike them down as unconstitutional or that there were adequate safeguards to prevent misuse.

The aforementioned cases will not apply in the backdrop of the Aadhaar program because they were rendered broadly in the context of prevention of crime. It needs no reiteration that an entire population cannot be presumed to be siphoning huge sums of money in welfare schemes or viewed through the lens of criminality, and therefore, considered as having a diminished expectation of privacy. The judgments cited by the respondents which were decided in the context of crime, require the State to at least form a reasonable belief about the criminal antecedents of individuals or their potential to commit crimes. On the contrary, by collecting identity information, the Aadhaar program treats every citizen as a potential criminal without even requiring the State to draw a reasonable belief that a citizen might be perpetrating a crime or an identity fraud. When the State is not required to have a reasonable belief and judicial determination to this effect, a program like Aadhaar, which infringes on the justifiable expectations of privacy of citizens flowing from the Constitution, is completely disproportionate to the objective sought to be achieved by the State.

218 The fundamental precepts of proportionality, as they emerge from decided cases can be formulated thus:

1. A law interfering with fundamental rights must be in pursuance of a legitimate state aim;
2. The justification for rights-infringing measures that interfere with or limit the exercise of fundamental rights and liberties must be based on the existence of a rational connection between those measures, the situation in fact and the object sought to be achieved;
3. The measures must be necessary to achieve the object and must not infringe rights to an extent greater than is necessary to fulfil the aim;
4. Restrictions must not only serve a legitimate purposes; they must also be necessary to protect them; and
5. The State must provide sufficient safeguards relating to the storing and protection of centrally stored data. In order to prevent arbitrary or abusive interference with privacy, the State must guarantee that the collection and use of personal information is based on the consent of the individual; that it is authorised by law and that sufficient safeguards exist to ensure that the data is only used for the purpose specified at the time of collection. Ownership of the data must at all times vest in the individual whose data is collected. The individual must have a right of access to the data collected and the discretion to opt out.

219 Privacy and proportionality are two interlocking themes that recur consistently in the above judgements. Privacy, also construed as “informational self-determination”, is a fundamental value. There is a consistent emphasis on the impact on personal dignity if private information is widely available and individuals are not able to decide upon its disclosure and use. This right of controlling the extent of the availability and use of one’s personal data is seen as a building block of data protection - especially in an environment where the state of technology facilitates ease of collection, analysis and dissemination of information.

220 The blanket and indiscriminate collection of information is seen as a violation of privacy, which is a constituent of the right to liberty. An extensive power to retain collected data is also seen as a disproportionate interference with the right to privacy and not necessary in a democratic society. The judgments hold that unlimited data retention and unrestricted state access both constitute a disproportionate interference with privacy and data protection. They also emphasize the need to clearly stipulate the nature of the data being collected and ensure its confidentiality. Provisions where these principles are not respected cannot be regarded as valid. While courts do recognize the need for public order and security, they emphasize the need to strike a balance between safeguarding public order and the right to privacy.

221 The principle of proportionality also recurs through these judgments, which note that the collection and use of information must be limited to the purpose specified by law and to the extent indispensable for the protection of public interest. The striking of a balance between public and private interests is crucial to proportionality. The judgments hold that there must be a protection against unauthorized use and clearly defined conditions for processing of data collected. Those conditions must not be excessive and must be justified on grounds of public interest and implemented in a manner proportionate to the objective. Too broad a scope of data collected and retained, the lack of limits imposed on access to data by authorities and a failure to distinguish between the treatment of data based on its usefulness and relevance are seen by Courts as constituting grounds for striking down the measure. While the State's imperatives are seen as relevant, emphasis is laid on retention and access requirements being proportionate to those imperatives and the need to prevent against abuse. Courts have upheld regulations that are necessary to achieve the legitimate aims and not excessive in their nature or impact.

The issue is whether the Aadhaar project and the Act, Rules and Regulations meet the test of proportionality.

H.4 Aadhaar: the proportionality analysis

222 Under Aadhaar, the State has put forth an objective of transferring subsidies and entitlements to its citizens. The aim was to curb leakages and to increase transparent and efficient “targeted delivery of subsidies, benefits and services”. However, the Act in the present form has surpassed a tailored objective and has sought to administer every facet of the citizen-state engagement through mandatory biometric-enabled Aadhaar linking. The violations of fundamental rights that result from the operation of the Aadhaar scheme will have to be evaluated on the touchstone of legitimate state interest and proportionality.

Since biometric systems have been employed, it is fundamental to understand that the right to privacy and its protection must be at the centre of the debate, from the very onset of the decision to use biometric data. It is vital that adequate safeguards are set down for every step of the process from collection to retention of biometric data. At the time of collection, individuals must be informed about the collection procedure, the intended purpose of the collection, the reason why the particular data set is requested and who will have access to their data. Additionally, the retention period must be justified and individuals must be given the right to access, correct and delete their data at any point in time, a procedure familiar to an opt-out option. The intended purpose should always act as a shining light and adequate caution must be

taken to ensure that there is no function creep with the lapse of time, in order to prevent the use of the data for new, originally unintended purposes. Measures to protect privacy would include enacting more entrenched and specific legislation so that the right to privacy is not only recognized but protected in all its aspects. Meeting this obligation would necessarily mean enactment of data protection legislation as well. The choice of particular techniques and the role of components in the architecture of the technology also have a strong impact on the privacy protections provided by the biometric system.

During the course of the hearing, the CEO of UIDAI, Mr Ajay Bhushan Pandey was permitted on the request of the learned Attorney General to make a power-point presentation before the Court, explaining the architecture and working of the Aadhaar project. On the basis of the presentation, Mr Shyam Divan, counsel for the petitioners had served a list of questions to the respondents. Responses to these questions have been filed by UIDAI. Analysing the power-point presentation by the CEO, questions addressed by Mr Divan and the responses filed by the respondents will facilitate an understanding of the architecture of the Aadhaar project.

Our analysis indicates that 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. UIDAI does not take

institutional responsibility for the correctness of the information entering its database. It delegates this task to the enrolment agency or the Registrar. The following response has been submitted by the respondents to the queries addressed specifically on this aspect:

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

223 UIDAI does not identify the persons who enrol within the Aadhaar system. Once the biometric information is stored in the CIDR during enrolment, it is only matched with the information received at the time of authentication. Biometric authentication of an Aadhaar number holder is performed as a "one to one" biometric match against the biometric information of the Aadhaar number holder in CIDR. Based on the match, UIDAI provides a 'yes' or 'no'response. Whether the information which is entering into CIDR is correct or not is a task entrusted to the enrolling agency or the Registrars. UIDAI does not assume responsibility for it.

The task of verifying whether a person is an illegal resident has also been left to the enrolling agencies. At the stage of enrolment, a verification of whether a person has been residing in India for 182 days or more in the past twelve months is done on the basis of a 'self-declaration' of the individual. The declaration which has been provided in the Aadhaar enrolment forms is thus:

> "Disclosure under section 3(2) of The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Servìces Act, 2016
> I confirm that I have been residing in India for at least 182 days in the preceding 12 months & information (including biometrics) provided by me to the UIDAI Ìs my own and is true, correct and accurate. I am aware that my information including biometrics will be tested for generation of Aadhaar and authentication. I understand that my identity information (except core biometric) may be provided to an agency only with my consent during authentication or as per the provisions of the Aadhaar Act. I have a right to access my identity information (except core biometrics) following the procedure laid down by UIDAI."[422]

224 The petitioners have argued that persons who were enrolled under the Aadhaar programme before the Act came into force on 12 September 2016 (more than a hundred crore) were not even required to make this declaration. The authenticity of the documents submitted (along with the declaration) is not checked by UIDAI.

The exception handling process permitting the use of alternative modes of identification if the Aadhaar authentication fails, is also left to the discretion of the Requesting Entity. On this aspect, the response which has been provided to the Court is thus:

> "As per Regulation 14(i) of Aadhaar (Authentication) Regulations 2016, requesting entities shall implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication services to Aadhaar number holders. Therefore, this exception handling mechanism is to be implemented and monitored by the requesting entities and in case of the government, their respective ministries."

Forty-nine thousand enrolment operators have been blacklisted by UIDAI. In reply to the question of the petitioners asking the reasons for blacklisting of the enrolment operators, UIDAI has stated that a data quality check is done during the enrolment process and if any Aadhaar enrolment is found to be not to be compliant with the UIDAI process, the enrolment gets rejected and an Aadhaar number is not generated. An operator who crosses a threshold defined in the policy, is blacklisted/ removed from the UIDAI ecosystem. UIDAI has provided information that forty-nine thousand operators were blacklisted/removed from the UIDAI ecosystem for the following reasons: (a) illegally charging residents for Aadhaar enrolment; (b) poor demographic data quality; (c) invalid biometric exceptions; and (d) other process malpractices. Once an operator is blacklisted or suspended, further enrolments cannot be carried out by it until the order of blacklisting/suspension is valid.

225 The Aadhaar architecture incorporates the role of Authentication User Agencies (AUAs) and Authentication Service Agencies (ASAs). ASAs, under the Aadhaar (Authentication) Regulations, have been defined as entities providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by UIDAI.[423] AUAs have been defined under the Aadhaar (Authentication) Regulations as requesting entities that use the Yes/No authentication facility provided by UIDAI.[424] "Yes/No

[423] Regulation 2(f), Aadhaar (Authentication) Regulations
[424] Regulation 2(g), Aadhaar (Authentication) Regulations

authentication facility" is a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, are matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing a "Yes" or "No", along with other technical details related to the authentication transaction, excluding identity information.[425] The other type of authentication facility is the e-KYC authentication facility, in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, are matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction. A requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by UIDAI is called a "e-KYC User Agency" or "KUA".[426] Under Regulation 15(2), a requesting agency may permit any other agency or entity to perform Yes/ No authentication by generating and sharing a separate license key for every such entity through the portal provided by UIDAI to the said requesting entity. It has also been clarified that sharing of a license key is only permissible for performing Yes/ No authentication, and is prohibited in case of e-KYC authentication.[427]

[425] Regulation 2(p), Aadhaar (Authentication) Regulations
[426] Regulation 2(l), Aadhaar (Authentication) Regulations
[427] Regulation 15, Aadhaar (Authentication) Regulations

The petitioners have contended that the points of service (PoS) biometric readers are capable of storing biometric information. The response which UIDAI has provided is extracted below:

> "UIDAI has mandated use of Registered Devices (RD) for all authentication requests. With Registered Devices biometric data is signed within the device/ RD service using the provider key to ensure it is indeed captured live. The device provider RD Service encrypts the PID block before returning to the host application. This RD Service encapsulates the biometric capture, signing and encryption of biometrics all within it. Therefore, introduction of RD in Aadhaar authentication system rules out any possibility of use of stored biometric and replay of biometrics captured from other source. Requesting entities are not legally allowed to store biometrics captured for Aadhaar authentication under Regulation 17(1)(a) of Aadhaar (Authentication) Regulations 2016."

226 A PID block is defined in Regulation 2(n) of Aadhaar (Authentication) Regulations, 2016 as the Personal Identity Data element, which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication. Regulation 17(1)(c) allows the requesting entity to store the PID block when "it is for buffered authentication where it may be held temporarily on the authentication device for a short period of time, and that the same is deleted after transmission". Thus, under the Aadhaar project, requesting entities can hold the identity information of individuals, even if for a temporary period.

It was further contended by the petitioners that authentication entities in the Aadhaar architecture are capable of recording the date and time of the authentication, the client IP, the device ID and purpose of authentication. In

response, UIDAI stated that it does not ask requesting entities to maintain any logs related to the IP address of the device, GPS coordinates of the device and purpose of authentication. It was, however, admitted that in order to ensure that their systems are secure and frauds are managed, AUAs like banks and telecom providers may store additional information according to their requirement to secure their system.

227 The process of sending authentication requests has been dealt with in Regulation 9 of the Aadhaar (Authentication) Regulations. It provides that after collecting the Aadhaar number or any other identifier provided by the requesting entity which is mapped to the Aadhaar number and necessary demographic and / or biometric information and/ or OTP from the Aadhaar number holder, the client application immediately packages and encrypts the input parameters into the PID block before transmission and sends it to the server of the requesting entity using secure protocols. After validation, the server of a requesting entity passes the authentication request to the CIDR, through the server of the Authentication Service Agency. The Regulation further provides that the authentication request must be digitally signed by the requesting entity and/or by the Authentication Service Agency, pursuant to the mutual agreement between them. Based on the mode of authentication requested, the CIDR validates the input parameters against the data stored and returns a digitally signed Yes or No authentication response, or a digitally signed e-KYC authentication response with encrypted e-KYC data, as the

case may be, along with other technical details related to the authentication transaction. In all modes of authentication, the Aadhaar number is mandatory and is submitted along with the input parameters such that authentication is always reduced to a 1:1 match. Clause (5) of Regulation 9 provides that a requesting entity shall ensure that encryption of PID Block takes place at the time of capture on the authentication device according to the processes and specifications laid down by UIDAI. Regulation 18(1) provides that a requesting entity would maintain logs of the authentication transactions processed by it, containing the following transaction details:

(a) the Aadhaar number against which authentication is sought;

(b) specified parameters of authentication request submitted;

(c) specified parameters received as authentication response;

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

(e) record of consent of the Aadhaar number holder for authentication.

The provision excludes retention of PID information in any case. Regulations 18(2) and 18(3) allow the retention of the logs of authentication transactions by the requesting entity for a period of two years. Upon the expiry of two years the logs have to be archived for a period of five years or the number of years required by the laws or regulations governing the entity, whichever is later. Upon the expiry of this period, the logs shall be deleted except those records which are required to be retained by a court or for any pending disputes. Regulation 20(1) provides that an Authentication Service Agency would

maintain logs of the authentication transactions processed by it, containing the following transaction details:

(a) identity of the requesting entity;

(b) parameters of authentication request submitted; and

(c) parameters received as authentication response.

The Regulation excludes retention of Aadhaar number, PID information, device identity related data and e-KYC response data. Under Regulations 20(2) and 20(3), authentication logs shall be maintained by the ASA for a period of two years, during which period the Authority and/or the requesting entity may require access to such records for grievance redressal, dispute redressal and audit in accordance with the procedure specified in the regulations. The authentication logs shall not be used for any purpose other than that stated. Upon the expiry of the period of two years, the authentication logs shall be archived for a period of five years. Upon the expiry of five years or the number of years required by the laws or regulations governing the entity whichever is later, the authentication logs shall be deleted except those logs which are required to be retained by a court or for pending disputes. Section 2(d)[428] of the Aadhaar Act allows storage of the record of the time of authentication. These provisions permit the storage of logs of authentication transactions for a specific time period.

The power-point presentation made by the CEO of UIDAI states that:

[428] Section 2(d) states: “authentication record” means the record of the time of authentication and identity of the requesting entity and the response provided by the Authority

> "With registered devices every biometric device will have a unique identifier allowing traceability, analytics and fraud management and biometric data will be signed within the device."

The response further indicates that UIDAI gets the AUA code, ASA code, unique device code, registered device code used for authentication, and that UIDAI would know from which device the authentication has happened and through which AUA/ASA. The response provided by the respondents states:

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

However, Regulation 26, which deals with the storage and maintenance of Authentication Transaction Data clearly provides that UIDAI shall store and maintain authentication transaction data, which shall contain the following information:

(a) authentication request data received including PID block;

(b) authentication response data sent;

(c) meta data[429] related to the transaction; and

(d) any authentication server side configurations[430] as necessary.

[429]AUA code, ASA code, unique device code, registered device code used for authentication, and that UIDAI would know from which device the authentication has happened

[430]An important configuration could be IP address

The only data, which has been excluded from retention under this provision, like Section 32(3) of the Aadhaar Act, is the purpose of authentication. Regulation 27 provides that the authentication transaction data shall be retained by UIDAI for a period of six months, and will thereafter be archived for five years, upon which, the authentication transaction data shall be deleted except when it is required to be maintained by a court or in connection with any pending dispute. These provisions indicate that under the Aadhaar architecture, UIDAI stores authentication transaction data. This is in violation of the widely recognized data minimisation principles which seek that data collectors and processors delete personal data records when the purpose for which it has been collected is fulfilled. The lack of specification of security standards and the overall lack of transparency and inadequate grievance redressal mechanism under the Aadhaar program greatly exacerbate the overall risk associated with data retention. In the Aadhaar regime, an Authentication User Agency (AUA) connects to the CIDR and uses Aadhaar authentication to validate a user and enable its services. The responsibility for the logistics of service delivery rests with the AUAs. In this federated model, Authentication Service Agencies (ASAs) transmit authentication requests to CIDR on behalf of one or more AUAs. However, any device that communicates via the Internet is assigned an IP address. Using the meta-data related to the transaction, the location of the authentication can easily be traced using the IP address.

228 The petitioners have also brought the attention of this Court to bear on an expert report, with respect to security and Aadhaar, which was filed along with an Additional Affidavit dated 09 March 2018. The report dated 4 March 2018 is titled as **"Analysis of Major Concern about Aadhaar Privacy and Security**" and has been authored by Professor Manindra Agrawal. Professor Agrawal is the N Ramarao Professor at IIT Kanpur and is a member of the Technology and Architecture Review Board (TARB) and of the Security Review Committee of UIDAI. Professor Agarwal's Report deals with the notion of *differential privacy*. Differential privacy makes it possible for tech entities to collect and share aggregate information about user habits, while maintaining the privacy of individual users. The Report states that differential privacy of a protocol is the change in the privacy of people when the protocol is introduced without altering any other protocol present. If the differential privacy of a protocol is "non-negative", the protocol does not compromise privacy in any way. There are four existing Aadhaar databases:

(i) The 'person database' stores personal attributes of a person (name, address, age, etc.) along with his/her Aadhaar number;

(ii) The reference database stores the Aadhaar number of a person along with a unique reference number (which has no relationship with the Aadhaar number of an individual);

(iii) The biometric database stores biometric information of a person along with the unique reference number; and

(iv) The verification log records all ID verifications done in the past five years. For each verification, it stores the biometric data, Aadhaar number, and ID of the device on which verification was done.

The report analyses the situation if any of the databases gets leaked. The report remarks:

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

The Report underlines the importance of ensuring the security of verification logs in the Aadhaar database. The leakage of verification logs is capable of damaging the security and privacy of individuals since the report notes that from the verification log, it is possible to locate the places of transactions by an individual in the past five years. A breach in verification log would allow a third party to access the location of the transactions of an individual over the past five years. The report indicates that it is possible through the Aadhaar database to track the location of an individual. The Aadhaar database is different from other databases such as PAN Card or driving license. The Aadhaar database is universal and contains the biometrics of an individual. The threshold to scrutinize the effects of this database is therefore much higher as compared to that of other databases.

229 In **Puttaswamy**, Justice Kaul (in his concurring judgment) emphasized upon the concerns regarding surveillance of individuals. The learned Judge held:

> "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… One such technique being adopted by States is 'profiling'. The European Union Regulation of 2016 on data privacy defines 'Profiling' as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Such profiling can result in discrimination based on religion, ethnicity and caste."[431]

Justice Kaul also dealt with the need to regulate the conduct of private entities vis-a-vis profiling of individuals:

> "The capacity of non-State actors to invade the home and privacy has also been enhanced. Technological development has facilitated journalism that is more intrusive than ever before…[432]
> …[I]n this digital age, individuals are constantly generating valuable data which can be used by non-State actors to track their moves, choices and preferences. Data is generated not just by active sharing of information, but also passively… These digital footprints and extensive data can be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions and hence, is valuable information. This is the age of 'big data'. The advancement in technology has created not just new forms of data, but also new methods of analysing the data and has led to the discovery of new uses for data. The algorithms are more effective and the computational power has magnified exponentially."[433]

[431] Puttaswamy at para 585
[432] Puttaswamy at para 587
[433] Puttaswamy at para 588

230 Section 2(c) of the Aadhaar Act is capable of revealing the identity of an individual to UIDAI. Section 2(d) permits storage of record of the time of authentication. Through meta data and in the light of the observations made in the Professor Manindra Agarwal Report, it can easily be concluded that it is possible through the UIDAI database to track the location of an individual. Further, the verification logs reveal the details of transactions over the past five years. The verification logs are capable of profiling an individual. Details of the transaction include what the transaction was (whether authentication request was accepted/rejected), where it was sent from, and how it was sent. The only thing not stored in the transaction is its purpose.

231 The threat to privacy arises not from the positive identification that biometrics provide, but the ability of third parties to access this in an identifiable form and link it to other information, resulting in secondary use of that information without the consent of the data subject. This erodes the personal control of an individual over the uses of his or her information. The unauthorised secondary use of biometric data is perhaps the greatest risk that biometric technology poses to informational privacy.[434] The Manindra Agarwal Report acknowledges that the biometric database in the CIDR is accessible by third-party vendors providing biometric search and de-duplication algorithms. The other three databases are stored, in encrypted form, by UIDAI.

[434] Nancy Yue Liu, Bio-Privacy: Privacy Regulations and the Challenge of Biometrics, Routledge (2013) at page 76

In this regard, it would be necessary to deal with the Contract (dated 24 August 2010) signed between UIDAI and L1 Identity Solutions (the foreign entity which provided the source code for biometric storage). It has been submitted by the petitioners that the contract gives L1 Identity Solutions free access to all personal information about all residents in India. The contract specifies that UIDAI ('the purchaser') has the right in perpetuity to use all original newly created processes "identified" by M/S L-1 Identity Solutions "solely during execution" of the contract to the purchaser's unique specifications and which do not contain any pre-existing intellectual property right belonging to L-1 Identity Solutions.[435] UIDAI was provided the license of the software (proprietary algorithms) developed by L-1 Identity Solutions. However, it has been clarified in the Contract that:

> "The Contract and the licenses granted herein are not a sale of a copy of the software and do not render Purchaser the owner of M/S L-1 Identity Solutions Operating Company's proprietary ABIS and SDK software."[436]

The Contract authorises L-1 Identity Solutions to retain proprietary ownership of all intellectual property rights in and to goods, services and other deliverables to the purchaser under the Contract that are modifications or derivative works to their pre-existing technologies, software, goods, services and other works. If a modification or derivative work made by L-1 Identity Solutions or its consortium members contains unique confidential information of the purchaser, then, the contract provides that the former shall not further

[435] Clause 13.1 of the Contract
[436] Ibid

license or distribute such modification or derivative to any other customer or third party other than the purchaser without the purchaser's prior written permission.[437] Clause 13.3 provides:

> "M/S L-1 Identity Solutions Operating Company/ The team of M/S L-1 Identity Solutions Operating Company shall ensure that while it uses any software, hardware, processes, document or material in the course of performing the Services, it does not infringe the Intellectual Property Rights of any person and M/S L-1 Identity Solutions Operating Company shall keep the Purchaser indemnified against all costs, expenses and liabilities howsoever, arising out any illegal or unauthorized use (piracy) or in connections with any claim or proceedings relating to any breach or violation of any permission/license terms or infringement of any Intellectual Property Rights by M/S L-1 Identity Solutions Operating Company or the team of M/S L-1 Identity Solutions Operating Company during the course of performance of the Services. In case of infringement by M/S L-1 Identity Solutions Operating Company/ The team of M/S L-1 Identity Solutions Operating Company, M/S L-1 Identity Solutions Operating Company shall have sole control of the defense and all related settlement negotiations."

Clause 13.4 deals with information privacy. It provides:

> "M/S L-1 Identity Solutions Operating Company/ The team of M/S L-1 Identity Solutions Operating Company shall not carry any written/printed document, layout diagrams, floppy diskettes, hard disk, storage tapes, other storage devices or any other goods/material proprietary to Purchaser into/out of Datacenter Sites and UIDAI Locations without written permission from the Purchaser."

Clause 15, titled as "data and hardware", provides:

> "15.1 By virtue of this Contract, M/s L-1 Identity Solutions Operating Company/The team of M/s L-1 Identity Solutions Operating Company may have access to personal information of the Purchaser [UIDAI] and/or a third party or any resident of India, any other person covered within the ambit of any legislation as may be applicable. The purchaser shall have the sole ownership of and the right to use all such data in

[437] Ibid

> perpetuity including any data or other information pertaining to the residents of India that may be in the possession of M/s L-1 Identity Solutions Operating Company or the Tram of M/s L-1 Identity Solutions Operating Company in the course of performing.
> 15.2 The purchaser shall have the sole ownership of and the right to use, proprietary Biometric templates of residents of India as created and maintained by M/S L-1 Identity Solutions Operating Company in the course of performing the Services under this Contract. In the event of termination or expiry of contract, M/S L-1 Identity Solutions Operating Company shall transfer all the proprietary templates to UIDAI in an electronic storage media in a form that is freely retrievable for reference and usage in future.
> 15.3 The Data shall be retained by M/S L-1 Identity Solutions Operating Company not more than a period of 7 years as per Retention Policy of Government of India or any other policy that UIDAI may adopt in future."

Under the Contract, L-1 Identity Solutions retains the ownership of the biometric software. UIDAI has been given only the license to use the software. Neither the Central Government nor the 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. It has also been provided that L-1 Identity Solutions can be given access to the database of UIDAI and the personal information of any individual.

232 This Court in **Puttaswamy** had emphasized on the centrality of consent in protection of data privacy:

> "307…Apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual. This is evident from the emphasis in the European data protection regime on the centrality of consent. Related to the issue of consent is the requirement of transparency which requires a disclosure by the data recipient of information pertaining to data transfer and use."

Prior to the enactment of the Aadhaar Act, an individual had no right of informed consent. Without the consent of individual citizens, UIDAI contracted with L-1 Identity Solutions to provide any information to it for the performance of the Contract. It has been provided in the Contract that L-1 Identity Solutions would indemnify UIDAI against any loss caused to it. However, the leakage of sensitive personal information of 1.2 billion citizens, cannot be remedied by a mere contractual indemnity. The loss of data is irretrievable. In a digital society, an individual has the right to protect herself by maintaining control over personal information. The protection of data of 1.2 billion citizens is a question of national security and cannot be indemnified by a Contract.

233 Mr Shyam Divan, learned senior counsel for the petitioners, has also drawn the attention of this Court to the Memorandum of Understanding (MoU) signed between UIDAI and various entities for carrying out the process of enrolment. Before the enactment of the Aadhaar Act, UIDAI existed as an executive authority, under the erstwhile Planning Commission and then under the Union Ministry of Communications and Information Technology. Mr. Divan has argued that the activities of the private parties engaged in the process of enrolment had no statutory or legal backing. It was his contention that MOUs signed between UIDAI and Registrars are not contracts within the purview of Article 299 of the Constitution, and therefore, do not cover the acts done by

the private entities engaged by the Registrars for enrolment. In **Monnet Ispat and Energy Ltd** v **Union of India**[438], this Court had held:

> "290. What the appellants are seeking is in a way some kind of a specific performance when there is no concluded contract between the parties. **An MOU is not a contract, and not in any case within the meaning of Article 299 of the Constitution of India.**"[439]

The MoUs entered into by UIDAI do not fall within the meaning of Article 299 of the Constitution. There is no privity of contract between UIDAI and the Enrolling agencies.

234 This Court held in **Puttaswamy** that any law which infringes the right to privacy of an individual needs to have stringent inbuilt safeguards against the abuse of the process. The Aadhaar Act envisages UIDAI as the sole authority for the purpose of the Act. It entrusts UIDAI with a wide canvass of functions, both administrative and adjudicatory. It performs the functions of appointing enrolling agencies, registrars and requesting entities. Currently, there are 212 Registrars and 755 enrolling agencies in different states of the country.[440] Monitoring the actions of so many entities is not a task easily done. Responsibility has also been placed on UIDAI to manage and secure the central database of identity information of individuals. UIDAI is also required to ensure that data stored in CIDR is kept secure and confidential. It has been placed with the responsibility for the protection of the identity information of 1.2 billion citizens. UIDAI is entrusted with discretionary powers under the

[438] (2012) 11 SCC 1
[439] Ibid, at page 153
[440] As submitted by Mr Rakesh Dwivedi, learned senior counsel for the State of Gujarat

architecture of Aadhaar, including the discretion to share the personal information of any individual with the biometric service providers (BSPs) for the performance of contracts with them.

235 The proviso to Section 28(5) provides only for a request to UIDAI for access to information and does not make access to information a right of the individual. This would mean that it would be entirely upon the discretion of the UIDAI to refuse to grant access to the information once a request has been made. It is also not clear how a person is supposed to know that the biometric information contained in the database has changed if he/she does not have access to it. UIDAI is also empowered to investigate any breach under the Act, as a result of which any offence under the Act will be cognizable only if a complaint is filed by UIDAI. UIDAI is not an independent monitoring agency.

Under the Aadhaar architecture, UIDAI is the only authority which carries out all the functions, be it administrative, adjudicatory, investigative, or monitoring of the project. While the Act confers such major functions on UIDAI, it does not place any institutional accountability upon UIDAI to protect the database of citizens' personal information. The Act is silent on the liability of UIDAI and its personnel in case of non-compliance of the provisions of the Act or the regulations made under it. Under Section 23(2)(s) of the Act, UIDAI is required to establish a grievance redressal mechanism. Making the authority administering a project, also responsible for providing for the framework to

address grievances arising from the project, severely compromises the independence of the grievance redressal body.[441] Section 47 of the Act violates the right to seek remedy. Under Section 47(1), a court can take cognizance of an offence punishable under the Act only on a complaint made by UIDAI or any officer or person authorised by it. There is no grievance redressal mechanism if any breach or offence is committed by UIDAI itself. The law must specify who is to be held accountable. The Act lacks a mechanism through which any individual can seek speedy redressal for his/her data leakage and identity theft. Compensation must be provided for any loss of data of an individual. A stringent and independent redressal mechanism and options for compensation must be incorporated in the law. Section 47 is arbitrary as it fails to provide a mechanism to individuals to seek efficacious remedies for violation of their right to privacy. Whether it is against UIDAI or a private entity, it is critical that the individual retains the right to seek compensation and justice. This would require a carefully designed structure.[442]

236 An independent and autonomous authority is needed to monitor the compliance of the provisions of any statute, which infringes the privacy of an individual. A fair data protection regime requires establishment of an independent authority to deal with the contraventions of the data protection framework as well as to proactively supervise its compliance. The

[441] The Centre for Internet & Society, Salient Points in the Aadhaar Bill and Concerns, available at https://cis-india.org/internet-governance/salient-points-in-the-aadhaar-bill-and-concerns.

[442] Shankkar Aiyar, Aadhaar: A Biometric History of India's 12-Digit Revolution, Westland (2017), at pages 226-227

independent monitoring authority must be required to prescribe the standards against which compliance with the data protection norms is to be measured. It has to independently adjudicate upon disputes in relation to the contravention of the law. Data protection requires a strong regulatory framework to protect the basic rights of individuals. The architecture of Aadhaar ought to have, but has failed to embody within the law the establishment of an independent monitoring authority (with a hierarchy of regulators), along with the broad principles for data protection.[443] The principles should include that the means of collection of data are fair and lawful, the purpose and relevance is clearly defined, user limitations accompanied by intelligible consent requirements are specified and subject to safeguards against risks such as loss, unauthorised access, modification and disclosure.[444] The independent authority needs to be answerable to Parliament. In the absence of a regulatory framework which provides robust safeguards for data protection, the Aadhaar Act does not pass muster against a challenge on the ground of Article 14. The law fails to meet the norms expected of a data protection regime which safeguards the data of 1.2 billion Indians. The absence of a regulatory framework leaves the law vulnerable to challenge on the ground that it has failed to meet the requirements of fair institutional governance under the rule of law.

237 The scheme of the Aadhaar Act is postulated on the norms enunciated in Chapter VI for the protection of information and their enforcement under a

[443]Subhashis Banerjee, Architecture for privacy, The Indian Express (5 May 2018), available at https://indianexpress.com/article/opinion/columns/architecture-for-privacy-data-protection-facebook-india-united-states-5163819/

[444] Shankkar Aiyar, Aadhaar: A Biometric History of India's 12-Digit Revolution, Westland (2017), at page 226

regime of criminal offences and penalties under Chapter VII. Providing a regime under law for penalizing criminal wrongdoing is necessary. But, criminal offences are not a panacea for a robust regulatory framework under the auspices of an autonomous regulatory body. Violations in regard to the integrity of data may be incremental. Millions of data transactions take place in the daily lives of a community of individuals. Violations in regard to the integrity of data are numerous. Some of them may appear to be trivial, if looked at in isolation. However, cumulatively, these violations seriously encroach on the dignity and autonomy of the individual. A regime of criminal law may not in itself be adequate to deal with all these violations in terms of their volume and complexity. It is hence necessary that the criminal law must be supplemented by an independent regulatory framework. In its absence, there is a grave danger that the regime of data protection, as well as the administration of criminal justice will be rendered dysfunctional. Unfortunately, a regulatory framework of the nature referred to above is completely absent. UIDAI which is established and controlled by the Union Government possesses neither the autonomy nor the regulatory authority to enforce the mandate of the law in regard to the protection of data. The absence of a regulatory framework renders the legislation largely ineffective in dealing with data violations. Data protection cannot be left to an unregulated market place. Nor can the law rest in the fond hope that organized structures within or outside government will be self-compliant. The Aadhaar Act has manifestly failed in its legislative design to establish and enforce an autonomous

regulatory mechanism. Absent such a mechanism, the state has failed to fulfil the obligation cast upon it to protect the individual right to informational self-determination.

238 Section 33(2), which permits disclosure of identity information and authentication records in the interest of national security, specifies a procedure for oversight by a committee. However, no substantive provisions have been laid down as guiding principles for the oversight mechanism such as the principle of data minimisation.

239 Privacy concerns relating to the Aadhaar project have been the subject of wide ranging deliberation. Biometric data offers strong evidence of one's identity since it represents relatively unique biological characteristics which distinguish one person from another. As biometric data can be usually linked to only one individual it acts as a powerful, unique identifier that brings together disparate pieces of personal information about an individual. As a relatively unique identifier, biometric data not only allows individuals to be tracked, but it also creates the potential for the collection of an individual's information and its incorporation into a comprehensive profile. Central databases, data matching/linking and profiling are technical factors that facilitate 'function creep' (the slippery slope according to which information can be used for functions other than that for which it was collected). Privacy advocates believe that any identification scheme can be carried out with a

hidden agenda and that the slippery slope effect can be relevant to several factors such as motivations of governments and business, and on the existence of safeguards. The special nature of biometric data makes function creep more likely and even attractive. The legal measures possible to control function creep are still limited. However, there are several ways in which function creep can be curtailed. They include (i) limiting the amount of data that is collected for any stated purpose; (ii) enabling regulation to limit technological access to the system; (iii) concerted debates with all stakeholders and public participation; (iv) dispersion of multiple enablers for a system; and (v) enabling choices for user participation.

240 This Court held in **Puttaswamy** that a reasonable expectation of privacy requires that data collection must not violate the autonomy of an individual. The Court has held consent, transparency, and control over information as the cornerstones over which the fundamentals of informational privacy stand. The Court had made it clear that an individual has the right to prevent others from using his or her image, name and other aspects of personal life and identity for commercial purposes without consent. An Aadhaar number is a unique attribute of an individual. It embodies unique information associated with an individual. The manner in which it is to be used has to be dependent on the consent of the individual.

241 Section 57 of the Aadhaar Act allows the use of an Aadhaar number for establishing the identity of an individual "for any purpose" by the state, private entities and persons. Allowing private entities to use Aadhaar numbers will lead to commercial exploitation of an individual's personal data without his/her consent and could lead to individual profiling. The contention is that Section 57 fails to meet the requirements set out in the **Puttaswamy** judgment.

In this regard, reference must be drawn to a 2010 policy paper. A group of officers was created by the Government of India to develop a framework for a privacy legislation that would balance the need for privacy protection with security and sectoral interests, and respond to the need for domain legislation on the subject. An approach paper for the legal framework for a proposed legislation on privacy was prepared by the group and was uploaded on the website of the Government of India. The paper noted the repercussions of having a project based on a database of unique individual IDs:

> "Data privacy and the need to protect personal information is almost never a concern when data is stored in a decentralized manner. However, all this is likely to change with the implementation of the UID Project. One of the inevitable consequences of the UID Project will be that the UID Number will unify multiple databases. As more and more agencies of the government sign on to the UID Project, the UID Number will become the common thread that links all those databases together. Over time, private enterprise could also adopt the UID Number as an identifier for the purposes of the delivery of their services or even for enrolment as a customer...Once this happens, the separation of data that currently exists between multiple databases will vanish…
>
> Such a vast interlinked public information database is unprecedented in India. It is imperative that appropriate steps be taken to protect personal data before the vast government

> storehouses of private data are linked up and the threat of data security breach becomes real."[445]

The Paper highlighted the potential of exploitation that the UID project possessed. The potential was that the UID data could be used directly or indirectly by market forces for commercial exploitation as well as for intrusions by the State into citizens' privacy. The Paper contained an incisive observation in regard to the exploitation of citizens' data by private entities:

> "Similarly, the private sector entities such as banks, telecom companies, hospitals etc are collecting vast amount of private or personal information about individuals. There is tremendous scope for both commercial exploitation of this information without the consent/ knowledge of the individual consent and also for embarrassing an individual whose personal particulars can be made public by any of these private entities. The IT Act does provide some safeguards against disclosure of data / information stored electronically, but there is no legislation for protecting the privacy of individuals for all information that may be available with private entities
>
> In view of the above, privacy of individual is to be protected both with reference to the actions of Government as well as private sector entities."[446]

The Paper highlighted the need for a stringent privacy protection mechanism, which could prevent individual data from commercial exploitation as well as individual profiling.

242 Reference must also be drawn to Chapter V of the National Identification Authority of India Bill, 2010, which provided for the constitution of

[445]Government of India, Approach Paper for a Legislation on Privacy (2010), available at http://www.prsindia.org/uploads/media/UID/aproach_paper.pdf
[446] Ibid

an Identity Review Committee. The proposed Committee was to be entrusted to carry out the function of ascertaining the extent and pattern of usage of Aadhaar numbers across the country. The Committee was required to prepare a report annually in relation to the extent and pattern of usage of the Aadhaar numbers along with its recommendations thereon and submit it to the Central Government. The idea behind the establishment of such a Committee was to limit the extent to which Aadhaar numbers could be used. These provisions have not been included in the Aadhaar Act, 2016. Instead, the Act allows the use of Aadhaar number for any purpose by the State as well as private entities. This is a clear case of overbreadth and an instance of manifest arbitrariness.

243 Section 57 indicates that the legislature has travelled far beyond its stated object of ensuring targeted delivery of social welfare benefits. Allowing the Aadhaar platform for use by private entities overreaches the purpose of enacting the law. It leaves bare the commercial exploitation of citizens data even in purported exercise of contractual clauses. This will result in a violation of privacy and profiling of citizens.

An article titled "**Privacy and Security of Aadhaar: A Computer Science Perspective**"[447] underlines the risk of profiling and identification that is possible by the use of Aadhaar numbers. It states:

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

244 The risks which the use of Aadhaar "for any purpose" carries is that when it is linked with different databases (managed by the State or by private entities), the Aadhaar number becomes the central unifying feature that connects the cell phone with geo-location data, one's presence and movement with a bank account and income tax returns, food and lifestyle consumption with medical records. This starts a "causal link" between information which was usually unconnected and was considered trivial.[448] Thus, linking Aadhaar with different databases carries the potential of being profiled into a system, which could be used for commercial purposes. It also carries the capability of influencing the behavioural patterns of individuals, by affecting their privacy and liberty. Profiling individuals could be used to create co-relations between human lives, which are generally unconnected. If the

[447] Shweta Agrawal, Subhashis Banerjee, and Subodh Sharma, Privacy and Security of Aadhaar: A Computer Science Perspective, Economic & Political Weekly (16 September 2017), Vol. 52, available at https://www.epw.in/journal/2017/37/special-articles/privacy-and-security-aadhaar.html

[448] Nishant Shah, Digital Native: Cause an effect, The Indian Express (17 June 2018), available at https://indianexpress.com/article/technology/social/digital-native-cause-an-effect-5219977/

traces of Aadhaar number are left in every facet of human life, it will lead to a loss of privacy. The repercussions of profiling individuals were anticipated in 1966 by Alexander Solzhenitsyn in '*Cancer Ward*'[449]. His views are prescient to our age:

> "As every man goes through life he fills in a number of forms for the record, each containing a number of questions. A man's answer to one question on one form becomes a little thread, permanently connecting him to the local centre of personnel records administration. There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialised as elastic bands, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence… Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads…"

The invisible threads of a society networked on biometric data have grave portents for the future. Unless the law mandates an effective data protection framework, the quest for liberty and dignity would be as ephemeral as the wind.

245 A novelist's vision is threatening to become a reality in our times. Profiling can impact individuals and their behaviour. Since data collection records the preferences of an individual based on the entities which requested for proof of identity, any such pattern in itself is crucial data that could be used to predict the emergence of future choices and preferences of individuals.

[449] Aleksandr Solzhenitsyn, Cancer Ward, The Bodley Head (1968)

These preferences could also be used to influence the decision making of the electorate in choosing candidates for electoral offices. Such a practice would be unhealthy for the working of a democracy, where a citizen is deprived of free choice. In the modern digital era, privacy protection does not demand that data should not be collected, stored, or used, but that there should be provable guarantees that the data cannot be used for any purpose other than those that have been approved. In any of the programmes employed, it is imperative that the state takes strong data privacy measures to prevent theft and abuse. Moreover, it must be realized that an identification system like Aadhaar, which is implemented nationwide, will always be more prone to external threats. The State is always open to threat from its adversaries, and a national level identification system can become an easy target for anyone looking to cause serious damage as individuals' biometric credentials are at risk in the process. Therefore, it is vital that state action ascertain security vulnerabilities while developing an identification system. These issues have not been dealt with by the Aadhaar Act. There is currently limited legislative or other regulatory guidance to specify whether private or public organisations are prevented from sharing or selling biometric information to others. Section 57 cannot be applied to permit commercial exploitation of the data of individuals or to affect their behavioural patterns. Section 57 does not pass constitutional muster. It is manifestly arbitrary, suffers from overbreadth and violates Article 14.

246 At its core, the Aadhaar Act attempts to create a method for identification of individuals so as to provide services, subsidies and other benefits to them. The Preamble of the Act explains that the architecture of the Act seeks to provide “efficient, transparent and targeted delivery of subsidies, benefits and services” for which the expenditure is incurred from the Consolidated Fund to resident individuals. Section 7 of the Act makes the proof of possession of Aadhaar number or Aadhaar authentication as a mandatory condition for receipt of a subsidy, benefit or service, which incurs expenditure from the Consolidated Fund of India. The scope of Section 7 is very wide. It leaves the door open for the government to route more benefits, subsidies and services through the Consolidated Fund of India and expand the scope of Aadhaar. Any activity of the government paid for from the Consolidated Fund of India ranging from supply of subsidised grains and LPG, to use of roads and civic amenities, healthcare, and even rebates to tax payers could come under such an umbrella. The scope of Section 7 could cover every basic aspect of the lives of citizens. The marginalized sections of society, who largely depend upon government’s social security schemes and other welfare programmes for survival could be denied basic living conditions because of a mismatch in biometric algorithms. The notifications issued by government under Section 7 of the Act, which require mandatory proof of possession of an Aadhaar number or requiring authentication, cover 252 schemes, including schemes for children (such as benefits under the Sarva Shiksha Abhiyan or getting meals under the Mid-day meal scheme, painting

and essay competitions for children, scholarships on merit), schemes relating to rehabilitation of bonded labour and human trafficking, scholarship schemes for SC/ST students, universal access to tuberculosis care, pensions, schemes relating to labour and employment, skill development, personnel and training, agriculture and farmers' welfare, primary and higher education, social justice, benefits for persons with disabilities, women and child development, rural development, food distribution, healthcare, panchayati raj, chemicals & fertilizers, water resources, petroleum and natural gas, science and technology, sanitation, textiles, urban development, minority affairs, road transport, culture, tourism, urban housing, tribal affairs and stipends for internship for students. The list is ever expanding and is endless. These notifications cover a large number of facilities provided by the government to its citizens. Every conceivable facility can be brought under the rubric of Section 7. From delivery to deliverance, almost every aspect of the cycle of life would be governed by the logic of Aadhaar.

247 When Aadhaar is seeded into every database, it becomes a bridge across discreet data silos, which allows anyone with access to this information to re-construct a profile of an individual's life. It must be noted while Section 2(k) of the Aadhaar Act excludes storage of individual information related to race, religion, caste, tribe, ethnicity, language, income or medical history into CIDR, the mandatory linking of Aadhaar with various schemes allows the same result in effect. For instance, when an individual from a particular caste

engaged in manual scavenging is rescued and in order to take benefit of rehabilitation schemes, she/he has to link the Aadhaar number with the scheme, the effect is that a profile as that of a person engaged in manual scavenging is created in the scheme database. The stigma of being a manual scavenger gets permanently fixed to her/his identity. What the Aadhaar Act seeks to exclude specifically is done in effect by the mandatory linking of Aadhaar numbers with different databases, under cover of the delivery of benefits and services.

Moreover, the absence of proof of an Aadhaar number would render a resident non-existent in the eyes of the State, and would deny basic facilities to such residents. Section 7 thus makes a direct impact on the lives of citizens. If the requirement of Aadhaar is made mandatory for every benefit or service which the government provides, it is impossible to live in contemporary India without Aadhaar. It suffers from the vice of being overbroad. The scope of subsidies provided by the government (which incur expenditure from the Consolidated Fund) is not the same as that of other benefits and services which the government provides to its citizens. Therefore, benefits and services cannot be measured with the same yardstick as subsidies. The inclusion of services and benefits in Section 7 is a pre-cursor to the kind of function creep which is inconsistent with privacy and informational self-determination. The broad definitions of the expressions ‘services and ‘benefits’ would enable government to regulate almost every

facet of its engagement with citizens under the Aadhaar platform. Section 7 suffers from clear overbreadth in its uncanalised application to services and benefits.

248 The open-ended nature of the provisions of Section 7 is apparent from the definition of 'benefit' in Section 2(f) and of 'service' in Section 2(w). 'Benefit' is defined to mean any advantage, gift, reward, relief or payment in cash or kind provided to an individual or a group of individuals. 'Service' is defined to mean any provision, facility, utility, or any other assistance provided in any form to an individual or a group of individuals. These are broad and unstructured terms under which the government can cover the entire gamut of its activities involving an interface with the citizen. The provision has made no requirement to determine whether in the first place biometric identification is necessary in each case and whether a less intrusive modality should suffice. Both the definitions include such other services as may be notified by the Central government. The residuary clause is vague and ambiguous and leaves it to the Central government at its uncharted discretion to expand on what benefits and services would be covered by the legislation. The manner in which these definitions have been expansively applied to cover a wide range of activities is attributable to the vagueness implicit in Section 7.

Can the provisions of Section 7 be applied with any justification to pensions payable on account of the past service rendered by a person to the state?

Pension, it is well settled, is not a largesse or bounty conferred by the state. Pension, as a condition of service, attaches as a recompense for the long years of service rendered by an individual to the state and its instrumentalities. Pensioners grow older with passing age. Many of them suffer from the tribulations of old age including the loss of biometrics. It is unfair and arbitrary on the part of the state to deny pension to a person entitled to it by linking pensionary payments to the possession of an Aadhaar number or to its authentication. A right cannot be denied on the anvil of requiring one and only one means of identification. The pension disbursing authority is entitled to lay down regulations (which are generally speaking, already in place) to ensure the disbursal of pension to the person who is rightfully entitled. This aim of the government can be fulfilled by other less intrusive measures. The requirement of insisting on an Aadhaar number for the payment of pensionary benefits involves a breach of the principle of proportionality. Such a requirement would clearly be contrary to the mandate of Article 14.

Similarly, the state as a part of its welfare obligations provides numerous benefits to school going children, including mid-day meals or scholarships, to children belonging to the marginalised segments of the society. Should the disbursal of these benefits be made to depend upon a young child obtaining an Aadhaar number or undergoing the process of authentication? The object of the state is to ensure that the benefits which it offers are being availed of by genuine students who are entitled to them. This legitimate aim can be fulfilled

by adopting less intrusive measures as opposed to the mandatory enforcement of the Aadhaar scheme as the sole repository of identification. The state has failed to demonstrate that a less intrusive measure other than biometric authentication will not subserve its purposes. That the state has been able to insist on adherence to the Aadhaar scheme without exception is a result of the overbreadth of Section 7. Consequently, the inclusion of benefits and services in Section 7 suffers from a patent ambiguity, vagueness and overbreadth which renders the inclusion of services and benefits arbitrary and violative of Article 14.

249 Various entities are involved in the Aadhaar project. Their inter-dependencies require a greater onus to be put on them so as to match privacy and security requirements. The architecture of Aadhaar treats individuals as data. However, the core must be about personhood. The architecture of Aadhaar is destroyed by a lack of transparency, accountability and limitations. Safeguards for protection of individual rights ought to have been explicitly guaranteed by design and default.[450] The presence of accountability and transparency within the Aadhaar architecture ought to be a necessary requirement so as to overcome the fear of the loss of privacy and liberty. Without these safeguards, the legislation and its architecture cannot pass muster under proportionality.

[450] Shankkar Aiyar, Aadhaar: A Biometric History of India's 12-Digit Revolution, Westland (2017), at page 226

It is also important to highlight that identity is a vital facet of personality and hence of the right to life under Article 21 of the Constitution. Identity is essential and inalienable to human relationships and in the dealings of an individual with the State. The notion that individuals possess only one, or at the least, a dominant identity is not sound constitutional principle. The Constitution has been adopted for a nation of plural cultures. It is accepting of diversity in every walk of life. Diversity of identity is an expression of the plurality which constitutes the essence of our social culture. Amartya Sen in '**The Argumentative Indian**'[451] demonstrates the untenability of the notion that identity is exclusive. He rejects the notion of an exclusive identity as "preposterous", observing that in different settings, individuals rely upon and assert varying identities:

> "Each of us invokes identities of various kinds in disparate contexts. The same person can be of Indian origin, a Parsee, a French citizen, a US resident, a woman, a poet, a vegetarian, an anthropologist, a university professor, a Christian, a bird watcher, and an avid believer in extra-terrestrial life and of the propensity of alien creatures to ride around the cosmos in multicoloured UFOs. Each of these collectivities, to all of which this person belongs, gives him or her a particular identity. They can all have relevance, depending on the context."[452]

Sen's logic, drawn from how individuals express their personalities in the real world, has a strong constitutional foundation. In the protection which it grants to a diverse set of liberties and freedoms, the Constitution allows for the assertion of different identities. The exercise of each freedom may generate a distinct identity. Combinations of freedoms are compatible with composite

[451] Amartya Sen, The Argumentative Indian, Penguin (2005), at page 350
[452] Ibid, at page 350

identities. Sen also rejects the notion that individuals "discover their identities with little room for choice". The support for such a notion, as he observes, comes from communitarian philosophy, according to which identity precedes choice:

> "As Professor Michael Sandel has explained this claim (among other communitarian claims) : 'community describes not just what they *have* as fellow citizens but also what they *are*, not a relationship they choose (as in a voluntary association) but an attachment they discover, not merely an attribute but a constituent of their identity In this view, identity comes *before* reasoning and choice."[453]

Sen rejects the above idea on the ground that it does not reflect a universally valid principle. Undoubtedly, some identities are 'given'. But even here, as Sen explains, the issue is not whether an identity can be selected by an individual in all cases but whether the individual has a choice over the relative weight to be ascribed to different identities:

> *"*The point at issue is not whether any identity whatever can be chosen (that would be an absurd claim), but whether we have choices over alternative identities or combinations of identities, and perhaps more importantly, whether we have some freedom in deciding what priority to give to the various identities that we may simultaneously have. People's choices may be constrained by the recognition that they are, say, Jewish or Muslim, but there is still a decision to be made by them regarding what importance they give to that particular identity over others that they may also have (related, for example, to their political beliefs, sense of nationality, humanitarian commitments or professional attachments)."[454]

Sen reasons that identity is a plural concept and the relevance of different identities depends on the contexts in which they are asserted:

[453] Ibid, at page 350
[454] Ibid, at page 351

> "Identity is thus a quintessentially plural concept, with varying relevance of different identities in distinct contexts. And, most importantly, we have choice over what significance to attach to our different identities. There is no escape from reasoning just because the notion of identity has been invoked. Choices over identities do involve constraints and connections, but the choices that exist and have to be made are real, not illusory. In particular, the choice of priorities between different identities, including what relative weights to attach to their respective demands, cannot be only a matter of discovery. They are inescapably decisional, and demand reason-not just recognition."[455]

250 The Constitution recognizes, through the rights which it protects, a multitude of identities and the myriad forms of its expression. Our political identities as citizens define our relationship with the nation state. The rights which the Constitution recognizes as fundamental liberties constitute a reflection of the identity of the self. As we speak, so we profess who we are. An artist who paints, the writer who shares a thought, the musician who composes, the preacher who influences our spirituality and the demagogue who launches into human sensibilities are all participants in the assertion of identity. In this participative process, the identities of both the performer and the audience are continuously engaged. Identity at a constitutional level is reflected in the entitlement of every individual, protected by its values, to lead a way of life which defines the uniqueness of our beings. The Constitution recognizes a multitude of identities, based on the liberties which it recognizes as an inseparable part of our beings. To be human is to have a multitude of identities and be guaranteed the right to express it in various forms. The state

[455] Ibid, at page 352

which must abide by a written Constitution cannot require any person to forsake one or more identities. Constitutional freedoms compel the state to respect them.

251 Technologies that affect how our identities function must be subject to constitutional norms. The existence of individual identity is the core of a constitutional democracy. Addressing the Constituent Assembly on 4th November 1948, Dr B.R. Ambedkar had emphasised on the importance of individual identity in our constitutional framework:

> "I am glad that the Draft Constitution has… adopted the individual as its unit."[456]

Having an individual identity is an important part of the human condition. The negation of identity is the loss of personhood, which in turn affects the freedom of choice and free will. Personhood constructs democracy. It represents the quality of democracy. Our decided cases have recognized the intimate relationship between human liberty and identity. The traveller in **Maneka Gandhi** v **Union of India**[457], the employee complaining of sexual harassment in **Vishaka** v **State of Rajasthan**[458], the guardian of the minor in **Githa Hariharan (Ms)** v **Reserve Bank of India**[459], the bar employee in **Anuj Garg** v **Hotel Association of India**[460], the transgender in **National Legal**

[456] Constituent Assembly Debates (4 November, 1948)
[457] (1978) 1 SCC 248
[458] (1997) 6 SCC 241
[459] (1999) 2 SCC 228
[460] (2008) 3 SCC 1

Services Authority v **Union of India**[461], the tribal worker in **Madhu Kishwar** v **State of Bihar**[462] and the oppressed victim of state violence in **Nandini Sundar** v **State of Chattisgarh**[463] are all engaged in the assertion of identity. **Puttaswamy** recognizes the role of the individual as "the core of constitutional focus" and "the focal point of the Constitution". Justice Kaul's concurring opinion recognised that the individual has the right to control her identity.[464]

It was submitted by the petitioners that a unique identity number infringes the identity of the individual since it reduces every resident to a number. Ascribing to the holder of an Aadhaar card, a unique identity number must not infringe constitutional identities. The Aadhaar Act indicates, in its Statement of Objects and Reasons, that correct identification of targeted beneficiaries is necessary and that a failure to establish the identity of an individual is a major hindrance in the disbursal of welfare benefits. Section 3(1) recognizes the entitlement of every resident to obtain an Aadhaar number. Section 4(3) provides that an Aadhaar number may be accepted as proof of identity. Section 7(1) indicates that its purpose is for establishing the identity of an individual for the receipt of services, benefits or subsidies drawn from the Consolidated Fund. These provisions cannot be allowed to displace constitutional identities. Nor can the provisions of Section 7 reduce an individual to a nameless or faceless person.

[461] (2014) 5 SCC 438
[462] (1996) 5 SCC 125
[463] (2011) 7 SCC 547
[464] Ibid

252 Aadhaar is about identification and is an instrument which facilitates a proof of identity. It must not obliterate constitutional identity. The definition of demographic information in Section 2(k) excludes race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history. However, as has been specifically discussed before, the linking of the Aadhaar number to different databases is capable of profiling an individual, which could include information regarding her/his race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history. Thus, the impact of technology is such that the scheme of Aadhaar can reduce different constitutional identities into a single identity of a 12-digit number and infringe the right of an individual to identify herself/himself with choice.

253 Social security schemes and programmes are a medium of existence of a large segment of society. Social security schemes in India, such as the PDS, were introduced to protect the dignity of the marginalized. Exclusion from these schemes defeats the rationale for the schemes which is to overcome chronic hunger and malnutrition. Exclusion is violative of human dignity. As discussed previously in detail, the statistics recorded in government records and the affidavits filed by the petitioners point out glaring examples of exclusion due to technical errors in Aadhaar. The authentication failures in the Aadhaar scheme have caused severe disruptions particularly in rural India. Exclusion as a consequence of biometric devices has a disproportionate impact on the lives of the marginalized and poor. This Court

cannot turn a blind eye to the rights of the marginalized. It may be the fashion of the day to advance the cause of a digital nation. Technology is undoubtedly an enabler. It has become a universal unifier of our age. Yet, the interface between technology and basic human rights cannot be oblivious to social reality. Compulsive linking of biometrics to constitutional entitlements should not result in denial to the impoverished. There exists a digital divide. To railroad those on one side of that divide unconcerned about social and technical constraints which operate in society is to defeat the purpose of social welfare. The Court has to be specifically conscious of the dignity of the underprivileged. The Court must fulfill its role of protecting constitutional values even if it affects a small percentage of the population. The exclusion errors in this case have led to grave injustice to the marginalized. The Court, therefore, has to play an active role in protecting their dignity.

254 The institution of rights places a heavy onus on the State to justify its restrictions. No right can be taken away on the whims and fancies of the State. The State has failed to justify its actions and to demonstrate why facilitating the targeted delivery of subsidies, which promote several rights such as the right to food for citizens, automatically entails a sacrifice of the right to privacy when both these rights are protected by the Constitution. One right cannot be taken away at the behest of the other especially when the State has been unable to satisfy this Court that the two rights are mutually exclusive. The State has been unable to respond to the contention of the

petitioners that it has failed to consider that there were much less rights-invasive measures that could have furthered its goals. The burden of proof on the State was to demonstrate that the right to food and other entitlements provided through the Aadhaar scheme could not have been secured without the violating the fundamental rights of privacy and dignity. Dworkin in his classical book "Taking Rights Seriously", while answering the question whether some rights are so important that the State is justified in doing all it can to maintain even if it abridges other rights, states that:

> "But no society that purports to recognize a variety of rights, on the ground that a man's dignity or equality may be invaded in a variety of ways, can accept such a principle… **If rights make sense, then the degrees of their importance cannot be so different that some count not at all when others are mentioned."**[465] (Emphasis supplied)

255 There is no antinomy between the right to privacy and the legitimate goals of the State. An invasion of privacy has to be proportional to and carefully tailored for achieving a legitimate aim. While the right to food is an important right and its promotion is a constitutional obligation of the State, yet the right to privacy cannot simply and automatically yield to it. No legitimate goal of the State can be allowed at the cost of infringement of a fundamental right without passing the test of constitutionality. While analysing the architecture of Aadhaar, this Court has demonstrated how the purported safeguards in the Aadhaar architecture are inadequate to protect the integrity of personal data, the right of informational self-determination and above all rights attributable to the privacy-dignity-autonomy trilogy. It is also concluded

[465] Ronald Dworkin, Taking Rights Seriously (1977), at pages 203-204

that the Aadhaar scheme is capable of destroying different constitutional identities. The financial exclusion caused due to errors in Aadhaar based authentication violate the individual's right to dignity. The Aadhaar scheme causes an unwarranted intrusion into fundamental freedoms guaranteed under the Indian Constitution since the respondents have failed to demonstrate that these measures satisfy the test of necessity and proportionality.

H.5 Dignity and financial exclusion

256 Our jurisprudence reflects a keen awareness of the need to achieve dignity. The nine judge Bench decision in **Puttaswamy** also emphasized the seminal value of dignity in our constitutional scheme. Human dignity is a strengthening bond in the relationship between Parts III and IV of the Constitution. Reading the Directive Principles contained in Part IV in the context of the right to life (in Part III of the Constitution) has significant implications both for the substantive content of the right and on the ability of the state in pursuit of its positive obligation to secure conditions of a dignified existence. Dignity is an integral element of natural law and an inalienable constitutional construct. To lead a dignified life is a constitutional assurance to an individual. Dr Ambedkar conceptualized four basic premises on which a political democracy can rest:

> "Political Democracy rests on four premises which may be set out in the following terms:

(i) The individual is an end in himself.
(ii) That the individual has certain inalienable rights which must be guaranteed to him by the Constitution.
(iii) **That the individual shall not be required to relinquish any of his constitutional rights as a condition precedent to the receipt of a privilege.**
(iv) **That the State shall not delegate powers to private persons to govern others.**"[466] (Emphasis supplied)

Interpreting the words of Dr Ambedkar in a constitutional context, any action on the part of the State which forces an individual to part with her or his dignity or any other right under Part III will not be permissible.

257 The experience of living with chronic hunger; recurring uncertainty about the availability of food; debt bondage; low and highly underpaid work; self-denial; and sacrifice of other survival needs, being discriminated against[467] are instances of the loss of dignity for the marginalized. The State has social security programmes and legislation to improve the living conditions of the marginalized and to protect their dignity and means of livelihood. However, as documented in the works of Sainath, Dreze, Sen and other authors, India has "utterly poor standards of the social services provided to common folk, whether it is the Mid-day Meal Scheme, the Sarva Shiksha Abhiyan, Integrated Child Development Services, Public Distribution system, healthcare at the primary health centres, district hospitals and even public

[466] Dr. Babasaheb Ambedkar: Writings and Speeches (Vol. 1), Dr. Ambedkar Foundation (2014)
[467] Harsh Mander, Living with Hunger: Deprivation among the Aged, Single Women and People with Disability, Economic & Political Weekly (April 26, 2008), Vol. 43, available at https://www.epw.in/journal/2008/17/special-articles/living-hunger-deprivation-among-aged-single-women-and-people

hospitals in the state capitals"[468]. This manner of addressing the deprivations faced by the marginalized crushes their dignity.

Any action or inaction on the part of the State which is insensitive to and unconcerned about protecting the dignity of the marginalized is constitutionally impermissible. Denial of benefits arising out of any social security scheme which promotes socio-economic rights of the marginalized, would not be legitimate under the Constitution, for the reason that such denial violates human dignity. No individual can be made to part with his or her dignity. Responsibility for protection of dignity lies not only with governments but also with individuals, groups and entities.

It is in the above background that this Court must deal with the next contention of the petitioners. The submission of the petitioners is that identity recognition technology may be based on a system which is deterministic or probabilistic. Biometric authentication systems work on a probabilistic model. For the purposes of authentication, a comparison is through a template which reduces the finger print to a scale and then, a minutea. The claim of the petitioners is that as a result, identities are reduced from certainty to a chance.

[468] Dignity, Not Mere Roti, Economic & Political Weekly (10 August, 2013), Vol. 48, available at https://www.epw.in/journal/2013/32/editorials/dignity-not-mere-roti.html

258 Section 7 of the Aadhaar Act makes it mandatory for an individual to undergo authentication or furnish proof of possession of an Aadhaar number in order to avail a subsidy, benefit or service, which incurs expenditure from the Consolidated Fund of India. In the Aadhaar based Biometric Authentication, the Aadhaar number and biometric information submitted by an Aadhaar number holder are matched with the biometric information stored in the CIDR. This may be fingerprints-based or iris-based authentication or other biometric modalities based on biometric information stored in the CIDR.[469]

It has been submitted that failure of the authentication process results in denial of a subsidy, benefit or service contemplated under Section 7 of the Act. It has been contended that non-enrolment in the Aadhaar scheme and non-linking of the Aadhaar number with the benefit, subsidy or service causes exclusion of eligible beneficiaries. It is the submission of the petitioners that authentication of biometrics is faulty, as biometrics are probabilistic in nature. It is the case of the petitioners that Aadhaar based biometric authentication often results in errors and thus leads to exclusion of individuals from subsidies, benefits and services provided under Section 7. Across the country, it has been urged, several persons are losing out on welfare entitlements because of a biometric mis-match. Mr Divan has argued in his written submissions, that “the project is not an ‘identity’ project but ‘identification’

[469] UIDAI, Aadhaar Authentication, available at https://uidai.gov.in/authentication.html

exercise and unless the biometrics work, a person in flesh and blood, does not exist for the state".

In order to deal with this contention, it is necessary to understand whether biometrics authentication can result in errors in matching. People are identified by three basic means: "by something they know, something they have, or something they are".[470] Biometrics fall within the last category, and, as such, should presumably be less susceptible to being copied or forged. However, various factors can reduce the probability of accurate human identification, and this increases the probability of a mismatch. Human fallibility can produce errors.[471]

259 In the United States of America, the National Academy of Science published a report in 2010 on biometrics titled "Biometric Recognition: Challenges & Opportunities"[472]. The report was based on a study carried out by several reputed scientists and researchers under the aegis of the National Research Council, the National Academy of Engineering and the Institute of Medicine. This report highlights the nature of biometrics as follows:

> "**Biometric recognition systems are inherently probabilistic** and their performance needs to be assessed within the context of this fundamental and critical characteristic. Biometric recognition involves matching, within

[470]United States General Accounting Office, Technology Assessment: Using Biometrics for Border Security (2002), available at http://www.gao.gov/new.items/d03174.pdf.
[471]Jeremy Wickins, The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification, Science & Engineering Ethics (2007), at pages 45-54
[472]Biometric Recognition: Challenges & Opportunities (Joseph N. Pato and Lynette I. Millett eds.), National Academy of Science- United States of America (2010), available at https://www.nap.edu/read/12720/chapter/1

> a tolerance of approximation, of observed biometric traits against previously collected data for a subject. Approximate matching is required due to the variations in biological attributes and behaviors both within and between persons."[473] (Emphasis supplied)

The report also took note of how changes in an individual's biometrics may occur due to a number of factors:

> "**Biometric characteristics and the information captured by biometric systems can be affected by changes in age, environment, disease, stress, occupational factors, training and prompting, intentional alterations, socio-cultural aspects of the situation in which the presentations occurs, changes in human interface with the system, and so on.** As a result, each interaction of the individual with the system (at enrolment, identification and so on) will be associated with different biometric information. Individuals attempting to thwart recognition for one reason or another also contribute to the inherent uncertainty in biometric systems."[474] (Emphasis supplied)

The report had also stated that biometrics can result in exclusion of people if it is used for claiming entitlement to a benefit:

> "**When used in contexts where individuals are claiming enrollment or entitlement to a benefit, biometric systems could disenfranchise people who are unable to participate for physical, social, or cultural reasons.** For these reasons, the use of biometrics—especially in applications driven by public policy, where the affected population may have little alternative to participation—merits careful oversight and public discussion to anticipate and minimize detrimental societal and individual effects and to avoid violating privacy and due process rights.
>
> Social, cultural, and legal issues can affect a system's acceptance by users, its performance, or the decisions on whether to use it in the first place—so it is best to consider these explicitly in system design. Clearly, the behavior of those being enrolled and recognized can influence the accuracy and effectiveness of virtually any biometric system,

[473] Ibid, at page 3
[474] Ibid

> and user behavior can be affected by the social, cultural, or legal context. Likewise, the acceptability of a biometric system depends on the social and cultural values of the participant populations."[475] (Emphasis supplied)

The report underlines that the relationship between an individual's biometric traits and data records has the potential to cause disenfranchisement, when a section of the population is excluded from the benefits of positive claim systems. The report thus states that:

> "Policies and interfaces to handle error conditions such as failure to enroll or be recognized should be designed to gracefully **avoid violating the dignity**, **privacy**, or due process rights of the participants." (Emphasis supplied)

260 Els Kindt in a comprehensive research titled "**Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis**"[476], deals with the nature of biometrics. The book notes that error rates in biometric systems lead to a situation where entitled data subjects will be falsely rejected from the process of database matching. This will adversely affect the rights of individuals. It has been observed that:

> "The error rates imply also that the system will allow impostors. This is equally important because the security of biometric systems should be questioned in case of high false accept rates. This element should be given sufficient weight in the decision to implement a biometric system for security purposes…
>
> Other tests clearly indicated increased error rates for young persons, in case of aging, in particular for face and for disabled persons. Individuals with health problems may also be falsely rejected or no longer be recognized, although they

[475] Ibid, at pages 10-11
[476] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, Springer (2013)

> were previously enrolled. In some cases, (non-)enrolment will be a significant problem. It is clear that these data subjects need additional protection."[477]

The book underlines the risk inherent in the limited accuracy of biometrics.[478]

261 A recently published book titled **"Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor"**[479], authored by Virginia Eubanks, deals with the impact of data mining, policy algorithms, and predictive risk models on economic inequality and democracy in America. Eubanks outlines the impacts of automated decision-making on public services in the USA through three case studies relating to welfare provision, homelessness and child protection services. Eubanks looks at these three areas in three different parts of the United States: Indiana, Los Angeles and Pittsburgh, to examine what technological automation has done in determining benefits and the problems it causes. The author records that in Indiana, one million applications for health care, food stamps, and cash benefits in three years were denied, because a new authentication system interpreted any application mistake as "failure to cooperate". In Los Angeles, an algorithm calculates the comparative vulnerability of thousands of homeless people so as to prioritize them for an inadequate pool of housing resources. In Pittsburgh, child services use an algorithm to predict future behaviour. Statistics are used to predict which children might be future victims of abuse

[477] Ibid, at page 363
[478] Ibid
[479] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, St. Martin's Press (2018)

or neglect. Eubanks shows how algorithms have taken over for human interaction and understanding. She has argued that automated decision-making is much wider in reach and is likely to have repercussions unknown to non-digital mechanisms, such as nineteenth-century poorhouses in America. Poorhouses were tax-supported residential institutions to which people were required to go if they could not support themselves.[480] People who could not support themselves (and their families) were put up for bid at public auction. The person who got the contract (which was for a specific time-frame) got the use of the labour of the poor individual(s) for free in return for feeding, clothing, housing and providing health care for the individual and his/her family. The practice was a form of indentured servitude and hardly had any recourse for protection against abuse. Eubanks considers the technology based decision-making for poverty management as the extension of the poorhouses of the 19th century:

> "America's poor and working-class people have long been subject to invasive surveillance, midnight raids, and punitive public policy that increase the stigma and hardship of poverty. During the nineteenth century, they were quarantined in county poorhouses. During the twentieth century, they were investigated by caseworkers, treated like criminals on trial. Today, we have forged what I call a digital poorhouse from databases, algorithms, and risk models. It promises to eclipse the reach and repercussions of everything that came before.
>
> Like earlier technological innovations in poverty management, digital tracking and automated decision-making hide poverty from the professional middle-class public and give the nation the ethical distance it needs to make inhuman choices: who gets food and who starves, who has housing and who remains homeless, and which families are broken by the state. The digital poorhouse is a part of a long American

[480] Tommy L. Gardner, Spending Your Way to the Poorhouse, Authorhouse (2004), at page 221

> tradition. We manage the individual poor in order to escape our shared responsibility for eradicating poverty."[481]

The author further remarks:

> "While poorhouses have been physically demolished, their legacy remains alive and well in the automated decision-making systems that encage and entrap today's poor. For all their high-tech polish, our modern systems of poverty management - automated decision-making, data mining, and predictive analysis - retain a remarkable kinship with the poorhouses of the past. Our new digital tools spring from punitive, moralistic views of poverty and create a system of high-tech containment and investigation. **The digital poorhouse deters the poor from accessing public resources; polices their labor, spending, sexuality, and parenting; tries to predict their future behavior; and punishes and criminalizes those who do not comply with its dictates. In the process, it creates ever-finer moral distinctions between the 'deserving' and 'undeserving' poor, categorizations that rationalize our national failure to care for one another.**"[482] (Emphasis supplied)

Eubanks builds the argument that automated decision-making technology does not act as a facilitator for welfare schemes for the poor and only acts as a gatekeeper:

> "New high-tech tools allow for more precise measuring and tracking, better sharing of information, and increased visibility of targeted populations. In a system dedicated to supporting poor and working-class people's self-determination, such diligence would guarantee that they attain all the benefits they are entitled to by law. In that context, integrated data and modernized administration would not necessarily result in bad outcomes for poor communities. But automated decision-making in our current welfare system acts a lot like older, atavistic forms of punishment and containment. It filters and diverts. It is a gatekeeper, not a facilitator."[483]

---

[481] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, St. Martin's Press (2018), at pages 12-13
[482] Ibid, at page 16
[483] Ibid, at pages 81-82

The crux of the book is reflected in the following extract:

> "We all live in the digital poorhouse. We have always lived in the world we built for the poor. We create a society that has no use for the disabled or the elderly, and then are cast aside when we are hurt or grow old. We measure human worth based only on the ability to earn a wage, and suffer in a world that undervalues care and community. We base our economy on exploiting the labor of racial and ethnic minorities, and watch lasting inequities snuff out human potential. We see the world as inevitably riven by bloody competition and are left unable to recognize the many ways we cooperate and lift each other up.
>
> **But only the poor lived in the common dorms of the county poorhouse. Only the poor were put under the diagnostic microscope of scientific clarity. Today, we all live among the digital traps we have laid for the destitute.**"[484] (Emphasis supplied)

Automating Inequality demonstrates the problems with authentication and algorithmic technology and indicates that the system, which was intended to provide assistance for the short term and help people out of poverty, has become a system to perpetuate poverty and injustice.

262 Errors in biometrics matching imply that an individual will not be considered a part of the biometrics database. If a benefit or service is subject to the matching of biometrics, then any mismatch would result in a denial of that benefit or service. Exclusion based on technological errors, with no fault of the individual, is a violation of dignity. The fate of individuals cannot be left to the vulnerabilities of technological algorithms or devices. 'To live is to live

[484] Ibid, at page 188

with dignity'.[485] Arbitrary exclusion from entitled benefits or subsidies is a violation of dignity. If any such project has to survive, then it has to be ensured that individual dignity is protected. These concerns have to be addressed.

As mentioned earlier, concerns regarding the application of biometrics in the Aadhaar project were discussed in 2009 by the Biometrics Standards Committee of UIDAI[486], which was of the view that the large magnitude of the Aadhaar project raised uncertainty about the accuracy of biometrics.[487] The Strategy Overview[488] published by UIDAI, in 2010, had discussed the risks associated with biometrics perceived by UIDAI itself. Under the heading of 'Project Risk', the overview stated the UID project does face certain risks in its implementation, which have to be addressed through its architecture and in the design of its incentives. It stated:

> "**1) Adoption Risks:** There will have to be sufficient, early demand from residents for the UID number. Without critical mass among key demographic groups (the rural and the poor) the number will not be successful in the long term. **To ensure this, the UIDAI will have to model de-duplication and authentication to be both effective and viable for participating agencies and service providers…**
>
> **3) Enrolment Risks:** The project will have to be carefully designed to address risks of low enrolment – such as creating sufficient touch points in rural areas, enabling and motivating Registrars, ensuring that documentary requirements don't derail enrolment in disadvantaged communities – as well as managing difficulties in address verification, name standards, lack of information on date of birth, and hard to record fingerprints.

[485] Puttaswamy, at para 119
[486] UIDAI Committee on Biometrics, Biometrics Design Standards For UID Applications, at page 4
[487] Ibid
[488] UIDAI, UIDAI Strategy Overview, (2010), available at http://www.prsindia.org/uploads/media/UID/UIDAI%20STRATEGY%20OVERVIEW.pdf

> **4) Risks of Scale: The project will have to handle records that approach one billion in number. This creates significant risks in biometric de-duplication as well as in administration, storage, and continued expansion of infrastructure.**
>
> **5) Technology risks**: Technology is a key part of the UID program, and this is the first time in the world that storage, authentication and de-duplication of biometrics are being attempted on this scale. **The authority will have to address the risks carefully – by choosing the right technology in the architecture, biometrics, and data management tools; managing obsolescence and data quality; designing the transaction services model and innovating towards the best possible result.**
>
> **6) Privacy and security risks**: The UIDAI will have to ensure that resident data is not shared or compromised."[489] (Emphasis supplied)

Technological error would result in authentication failures. The concerns raised by UIDAI ought to have been resolved before the implementation of the Aadhaar project. Poor connectivity in rural India was a major concern. The majority of the Indian population lives in rural areas. Even a small percentage of error results in a population of crores being affected. Denial of subsidies and benefits to them due to the infirmities of biometric technology is a threat to good governance and social parity.

263 The issue of exclusion needs to be considered at three different levels: (i) before the implementation of the Aadhaar Act, when biometrics were being used since 2009; (ii) under the provisions of the Act; and (iii) at the practical level during the implementation of the Aadhaar programme.

[489] Ibid, at page 38

Before the enactment of the Aadhaar Act in 2016, the Standing Committee on Finance, which examined the NIA Bill, was concerned about the impact of Aadhaar on marginalized sections of society. Since the availing of subsidies and benefits was to depend upon Aadhaar based authentication, any error in the authentication would result in a denial of the benefits of social security schemes for the marginalized. In 2011, the report of the Standing Committee noted, thus:

> "The full or near full coverage of marginalized sections for issuing Aadhaar numbers could not be achieved mainly owing to two reasons viz. (i) the UIDAI doesn't have the statistical data relating to them; and (ii) **estimated failure of biometrics is expected to be as high as 15% due to a large chunk of population being dependent on manual labour.**"[490] (Emphasis supplied)

The **Economic Survey 2016-17** has adverted to authentication failures while discussing the concept of Universal Basic Income (UBI). The Survey, which is an official document of the Union government, states that UBI is premised on the idea that a just society needs to guarantee to each individual a minimum income which they can count on, and which provides the necessary material foundation for a life with access to basic goods and a life of dignity.[491] UBI was to be implemented by providing cash transfers (for availing benefits of social security schemes) to the bank accounts of beneficiaries. The implementation of UBI was to be undertaken through what is described as the JAM trinity:

[490] Forty-Second Report of the Standing Committee on Finance (2011), available at http://www.prsindia.org/uploads/media/UID/uid%20report.pdf, at page 30

[491] Government of India, Economic Survey 2016-17, available at https://www.thehinducentre.com/multimedia/archive/03193/Economic_Survey_20_3193543a.pdf, at page 173

Jan-Dhan Bank Accounts, Aadhaar data and Mobile phones. However, the Survey noted that while Aadhaar is designed to solve the identification problem, it cannot solve the "targeting problem" on its own. The Survey emphasized the need to build state capacity and that "the state will still have to enhance its capacities to provide a whole range of public goods".[492] The Survey has recorded the statistics of authentication failures of Aadhaar in several regions of the country:

> "While Aadhaar coverage speed has been exemplary, with over a billion Aadhaar cards being distributed, some states report authentication failures: estimates include 49 percent failure rates for Jharkhand, 6 percent for Gujarat, 5 percent for Krishna District in Andhra Pradesh and 37 percent for Rajasthan. Failure to identify genuine beneficiaries results in exclusion errors."[493]

No failure rate in the provision of social welfare benefits can be regarded as acceptable. Basic entitlements in matters such as foodgrain, can brook no error. To deny food is to lead a family to destitution, malnutrition and even death.

264 A recent Office Memorandum dated 19 December 2017 issued by the Cabinet Secretariat of the Union government[494] acknowledges that the Aadhaar enrolment process has not been completed and that infrastructure constraints are capable of posing difficulties in online authentication. The Memorandum provides that those beneficiaries who do not possess Aadhaar,

[492] Ibid, at page 174
[493] Ibid, at page 194
[494] Office Memorandum dated 19 December 2017, available at https://dbtbharat.gov.in/data/om/Office%20Memorandum_Aadhaar.pdf

shall be provided a subsidy, benefit or service based on alternate identification documents as contemplated by Section 7 of the Aadhaar Act. It also requires efforts to be made to ensure that all beneficiaries are facilitated to get enrolment under the Aadhaar programme. The Memorandum creates a mechanism for availing subsidies, benefits or services in cases where Aadhaar authentication fails:

(i) Departments and Bank Branches may make provisions for IRIS scanners along with fingerprint scanners wherever feasible;

(ii) In cases of failure due to lack of connectivity, offline authentication systems such as QR code based coupons, Mobile based OTP or TOTP may be explored; and

(iii) In all cases where online authentication is not feasible, the benefit/service may be provided on the basis of possession of Aadhaar, after duly recording the transaction in a register, to be reviewed and audited periodically.

The figures from the Economic Survey of India indicate that there are millions of eligible beneficiaries across India who have suffered financial exclusion. The Cabinet Secretariat has pro-actively acknowledged the need to address matters of exclusion by implementing alternate modalities, apart from those set out in Section 7. Options (i) and (ii) above were to be implemented in future. This exercise should have been undertaken by the government in advance. Problems have to be anticipated when a project is on the drawing

board, not after severe deprivations have been caused by the denial of social welfare benefits.

265 Exclusion of citizens from availing benefits of social security schemes because of failures or errors in Aadhaar based biometric authentication has also been documented in research studies and academic writings published by members of civil society, including Reetika Khera and Jean Dreze. Similar testimonies have been recorded in affidavits submitted before this Court by civil society activists. Hearing the voices of civil society must be an integral part of the structural design of a project, such as Aadhaar. In the absence of a credible mechanism to receive and respond to feed-back, the state has to depend on its own personnel who may not always provide reliable and candid assessments of performance and failure.

266 ABBA (Aadhaar based biometric authentication) refers to the practice of installing a Point of Sale (PoS) machine equipped with a fingerprint reader and authenticating a person each time she accesses her entitlements.[495] Dreze has stated that for successful authentication in PDS outlets, several technologies need to work simultaneously.[496] These are[497]:

[495]Reetika Khera, Impact of Aadhaar on Welfare Programmes, Economic & Political Weekly, Vol. 52 (16 December 2017), available at https://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html

[496]Jean Dreze, Dark clouds over the PDS, The Hindu (10 September 2016), available at https://www.thehindu.com/opinion/lead/Dark-clouds-over-the-PDS/article14631030.ece

[497] Anmol Somanchi, Srujana Bej, and Mrityunjay Pandey, Well Done ABBA? Aadhaar and the Public Distribution System in Hyderabad, Economic & Political Weekly (18 February 2017), Vol. 52, available at https://www.epw.in/journal/2017/7/web-exclusives/well-done-abba.html

(a) **Seeding of Aadhaar numbers:** An eligible individual can become a beneficiary and access the PDS system only if her Aadhaar number is correctly seeded onto the PDS database and added to the household ration card;

(b) **Point of Sale (PoS) machines:** The process at the PDS outlet is dependent on the PoS machine. If it malfunctions, no transaction can be made. The first step in the process requires the dealer to enter the ration card number of the beneficiary's household onto the PoS machine;

(c) **Internet connection:** Successful working of the PoS machine depends on internet connectivity as verification of the ration card number and the beneficiary's biometric fingerprint is carried out over the internet;

(d) **Remote Aadhaar servers:** Remote Aadhaar servers verify the ration card number and initiate fingerprint authentication; and

(e) **Fingerprint recognition software:** The beneficiary proves her identity by submitting to fingerprint recognition in the PoS machine. Upon verification, the PoS machine indicates that the beneficiary is genuine and that foodgrains can be distributed to her household.

The above procedure requires that at the time of purchase of PDS grains each month, any one person listed on the ration card needs to authenticate themselves. Similarly, for pensions, elderly persons must go to the point of delivery to authenticate themselves. Reetika Khera has observed that since ABBA on PoS machines is currently a monthly activity, so each of its

associated technologies (correct Aadhaar-seeding, mobile connectivity, electricity, functional PoS machines and UIDAI servers and fingerprint recognition) needs to work for a person to get their entitlement.[498] Dreze has referred to the above procedure as "a wholly inappropriate technology for rural India"[499]. Network failures and other glitches routinely disable this sort of technology. Dreze has further observed that in villages with poor connectivity, it is a "recipe for chaos"[500].

267 A government-commissioned sample study[501] in Andhra Pradesh to ascertain the efficiency of Aadhaar-based social programmes in the case of subsidised grains indicated that technical deficiencies are depriving the poor of their access to food. The study was commissioned by the state government after it was found that 22% of the PDS beneficiaries did not take the ration in the month of May 2015. The sample study, which covered five PDS outlets in three districts, found that half of the beneficiaries of PDS in the surveyed areas could not access their ration quota due to glitches, lack of training and mismatches linked to Aadhaar. In the survey, a majority of beneficiaries reported fingerprint mismatches and the inability of fair-price shop owners to

[498]Reetika Khera, Impact of Aadhaar on Welfare Programmes, Economic & Political Weekly, Vol. 52 (16 December 2017), available at https://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html

[499]Jean Dreze, Dark clouds over the PDS, The Hindu (10 September 2016), available at https://www.thehindu.com/opinion/lead/Dark-clouds-over-the-PDS/article14631030.ece

[500]Ibid

[501]Society for Social Audit, Accountability and Transparency, FP Shops Left Over Beneficiaries Report, available at http://www.socialaudit.ap.gov.in/SocialAudit/LoadDocument?docName=Fair%20Price%20Work%20%20Shops%20(Ration%20Card%20Holders)%20-%20Beneficiaries%20Report.pdf&type=application. See also Aadhaar-based projects failing the poor, says Andhra govt study, Hindustan Times (7 October 2015), available at https://www.hindustantimes.com/india/aadhaar-based-projects-failing-the-poor-says-andhra-govt-study/story-7MFBCeJcfl85Lc5zztON6L.html

operate point-of-sale (POS) devices correctly as major hurdles. Aadhaar numbers did not match with ration card numbers in many cases.

Another survey[502] of 80 households conducted in Hyderabad finds that despite the introduction of technology-intensive authentication and payment systems, a significant number of those vulnerable and dependent on Public Distribution System (PDS) for food grains are failing to realise their right to food. The survey revealed that among 80 surveyed households, 89% reported receiving full entitlements at correct prices even before the introduction of Aadhaar-based biometric authentication (ABBA). In contrast, 10% of households were excluded due to authentication failures due to reported errors with one or more of its five technological components.

268 An article titled "**Aadhaar and Food Security in Jharkhand: Pain without Gain?**"[503], based on a household survey in rural Jharkhand, examines various issues related to compulsory ABBA for availing PDS benefits. The article notes the impact of PDS on the lives of the rural poor, who visit the ration shop every month. In "their fragile and uncertain lives", the PDS provides a "modicum of food and economic security". The article notes that in ABBA, the failure of authentication results in denial of food from ration shops. The household is unable to get food rations for no fault of its own. The

[502]Anmol Somanchi, Srujana Bej, and Mrityunjay Pandey, Well Done ABBA? Aadhaar and the Public Distribution System in Hyderabad, Economic & Political Weekly, Vol. 52 (18 February 2017), available at https://www.epw.in/journal/2017/7/web-exclusives/well-done-abba.html

[503]Jean Drèze, Nazar Khalid, Reetika Khera, and Anmol Somanchi, Aadhaar and Food Security in Jharkhand: Pain without Gain?, Economic & Political Weekly, Vol. 52 (16 December 2017).

article comes to the conclusion that the imposition of ABBA on the PDS in Jharkhand is a case of "pain without gain", as it has led to serious problems of exclusion (particularly for vulnerable groups such as widows, the elderly and manual workers). The article further notes that ABBA has neither failed to reduce quantity fraud (which is the main form of PDS corruption in Jharkhand), nor has it helped to address other critical shortcomings of the PDS in Jharkhand, such as the problem of missing names in ration cards, the identification of Antyodaya (poorest of the poor) households, or the arbitrary power of private dealers. The article identifies poor internet connectivity as one of the reasons for authentication failures and eventual exclusion:

> "Sporadic internet connectivity is another major hurdle. Sometimes, light rain is enough to disrupt connectivity or the electricity supply. Every step in the ABBA process—ration card verification, biometric authentication, electronic upload of transactions, updating NFSA [National Food Security Act] lists and entitlements on the PoS[504] [Point of Sale] machine—depends on internet connectivity. Further, even with stable connectivity, biometric authentication is not always easy. Biometric failures are especially common for two groups: the elderly, and manual labourers. Both are particularly vulnerable to food insecurity."[505]

The article regards the denial of basic services to the poor due to failure of ABBA as a form of grave injustice:

[504] Ibid, at page 51. The article states: "[PoS] is a handheld device installed at every PDS outlet ("ration shop") and connected to the Internet. The list of ration cards attached to that outlet, and their respective entitlements, are stored in the PoS machine and updated every month. When a cardholder turns ups, the PoS machine first "authenticates" her by matching her fingerprints with the biometric data stored against her Aadhaar number in the Central Identities Data Repository (CIDR). The machine then generates a receipt with the person's entitlements, which are also audible from a recorded message... The transaction details are also supposed to be entered by the dealer in the person's ration card."

[505] Ibid, at page 55

> "**Imposing a technology that does not work on people who depend on it for their survival is a grave injustice.**"[506] (Emphasis supplied)

As we have noted in an earlier part of this judgment, even the Economic Survey of India 2016-17 found a 49% failure rate for beneficiaries in Jharkhand and 37% in Rajasthan. Those at the receiving end are the poorest of the poor.

Reetika Khera looks at the impact of Aadhaar-integration with security schemes (primarily in MGNREGA, PDS and social security pensions).[507] The author also discusses briefly the impact of Aadhaar on liquefied petroleum gas (LPG) subsidy and the application of Aadhaar in the mid-day meal (MDM) scheme. In coming to its conclusions, the article has relied upon quantitative data from primary field studies, secondary data from government portals, figures obtained through queries made under the Right to Information (RTI) Act, and responses to questions in Parliament. In Khera's words, Aadhaar is becoming a "tool of exclusion":

> "**Savings or exclusion?** The government claimed that Aadhaar integration saved 399 crore up to 31 December 2016 (GoI 2017c). At a given level of benefits, a reduction in government expenditure in any particular transfer scheme can be on two counts: removal of ghosts and duplicates ("efficiency"); and a fall in the number of genuine beneficiaries ("shrinkage"), for instance, if they do not link their Aadhaar numbers when required. Across welfare schemes, the government has been treating *any* reduction in expenditure as "savings," even when it comes from shrinkage. This is true

[506] Ibid, at page 58

[507] Reetika Khera, Impact of Aadhaar on Welfare Programmes, Economic & Political Weekly, Vol. 52 (16 December 2017), available at https://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html

> for SSP [social security pension] as well. For instance, in Rajasthan, pensioners were "mistakenly" recorded as dead and this was presented as Aadhaar-enabled savings (Yadav 2016f). In Jharkhand too, pensioners' names have been deleted because they did not complete Aadhaar-seeding formalities or pensions stopped due to seeding errors (Sen 2017a). Studying 100 pensioners, selected from 10 randomly-selected villages from five blocks of Ranchi district in February 2017, Biswas (2017) finds that 84% of her respondents receive pensions but irregularity in payments was a big issue. The remaining 16% were not receiving it due to Aadhaar-related issues."[508]

Puja Awasthi documents the plight of individuals suffering from leprosy, who have been denied pensions due to not being able to get enrolled into the Aadhaar system. Leprosy can damage fingerprints and thus make an individual incapable of providing biometrics. Awasthi's article[509] notes that Aadhaar is capable of causing a denial of benefits or services to 86,000 citizens, who suffer from leprosy.

These writings show how in most cases, an authentication failure means that the individual/household was denied the benefit of a social security programme for no fault of their own. Some have gone hungry. Some reportedly lost their lives.[510]

[508] Ibid, at page 66

[509] Puja Awasthi, Good enough to vote, not enough for Aadhaar, People's Archive of Rural India, available at https://ruralindiaonline.org/articles/good-enough-to-vote-not-enough-for-aadhaar

[510] Yet another Aadhaar-linked death? Denied rations for 4 months, Jharkhand woman dies of hunger, Scroll (3 Feb. 2018), available at: https://scroll.in/article/867352/yet-another-aadhaar-linked-death-jharkhand-woman-dies-of-hunger-after-denial-of-rations; Denied food because she did not have Aadhaar-linked ration card, Jharkhand girl dies of starvation, Scroll (16 Oct 2017), available at: https://scroll.in/article/854225/denied-food-because-she-did-not-have-aadhaar-linked-ration-card-jharkhand-girl-dies-of-starvation

269 A person's biometrics change over time. For persons, who are engaged in manual labour, and persons who are disabled or aged, fingerprints actually cannot be captured by biometric devices. The material which has been relied upon in this segment originates from government's official documents as well as from distinguished academics and researchers from civil society. There exist serious issues of financial exclusion. Pensions for the aged particularly in cases where a pension is earned for past service – are not charity or doles. They constitute legal entitlements. For an old age pensioner, vicissitudes of time and age obliterate fingerprints. Hard manual labour severely impacts upon fingerprints. The elderly, the disabled and the young are the most vulnerable and a denial of social welfare entitlements verily results in a deprivation of the right to life. Should the scholarship of a girl child or a mid-day meal for the young be made to depend on the uncertainties of biometric matches? Our quest for technology should not be oblivious to the country's real problems: social exclusion, impoverishment and marginalisation. The Aadhaar project suffers from crucial design flaws which impact upon its structural probity. Structural design in delivering welfare entitlements must be compliant with structural due process, to be in accord with Articles 14 and 21. The Aadhaar project has failed to account for and remedy the flaws in its framework and design which lead to serious issues of exclusion. Dignity and rights of individuals cannot be based on algorithms or probabilities. Constitutional guarantees cannot be subject to the vicissitudes of technology.

270 Structural due process imposes requirements on public institutions and projects at the macro level. Structural due process requires that the delivery of social welfare benefits must be effective and timely. Those who are eligible for the benefits must not face exclusion. Procedures for the disbursal of benefits must not be oppressive. They must be capable of compliance both by those who disburse and by those who receive the benefits. Deployment of technology must factor in the available of technological resources in every part of the coverage area and the prevailing levels of literacy and awareness. Above all, the design of the project will be compliant with structural due process only if it is responsive to deficiencies, accountable to the beneficiaries and places the burden of ensuring that the benefits reach the marginalised on the state and its agencies.

H.6 Constitutional validity of Section 139AA of the Income Tax Act 1961

271 Section 139AA of the Income Tax Act 1961 which was inserted by the Finance Act 2017, mandates the quoting of an Aadhaar number in the application for a Permanent Account Number (PAN) and in the return of income tax. Failure to intimate an Aadhaar number results in the PAN being deemed invalid retrospectively.

Section 139AA reads thus:

> "**Quoting of Aadhaar number**.- (1) Every person who is eligible to obtain Aadhaar number shall, on or after the 1st day of July, 2017, quote Aadhaar number-
>
> (i) in the application form for allotment of permanent account number;

(ii) in the return of income:

Provided that where the person does not possess the Aadhaar Number, the Enrolment ID of Aadhaar application form issued to him at the time of enrolment shall be quoted in the application for permanent account number or, as the case may be, in the return of income furnished by him.

(2) Every person who has been allotted permanent account number as on the 1st day of July, 2017, and who is eligible to obtain Aadhaar number, shall intimate his Aadhaar number to such authority in such form and manner as may be prescribed, on or before a date to be notified by the Central Government in the Official Gazette:

Provided that in case of failure to intimate the Aadhaar number, the permanent account number allotted to the person shall be deemed to be invalid and the other provisions of this Act shall apply, as if the person had not applied for allotment of permanent account number.

(3) The provisions of this Section shall not apply to such person or class or classes of persons or any State or part of any State, as may be notified by the Central Government in this behalf, in the Official Gazette.

Explanation. - For the purposes of this section, the expressions –

(i) "Aadhaar number", "Enrolment" and "resident" shall have the same meanings respectively assigned to them in Clauses (a), (m) and (v) of Section 2 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

(ii) "Enrolment ID" means a 28 digit Enrolment Identification Number issued to a resident at the time of enrolment."

272 In **Binoy Viswam** v **Union of India ("Binoy Viswam")**,[511] a two judge Bench (consisting of Dr Justice AK Sikri and Justice Ashok Bhushan) upheld the constitutional validity of Section 139AA. Since the issue of whether privacy is a constitutionally guaranteed right was pending before a Bench of nine judges (the decision in **Puttaswamy** was still to be delivered), the two judge

[511] (2017) 7 SCC 59

Bench did not dwell on the challenge to the legislation on the ground of privacy and under Article 21. The Bench examined other submissions based on Articles 14 and 19 and on the competence of Parliament to enact the law.

273 The decision in **Binoy Viswam** holds that in assessing the constitutional validity of a law, two grounds of judicial review are available:

(i) The legislative competence of the law-making body which has enacted the law, over the subject of legislation; and

(ii) Compliance with Part III of the Constitution, which enunciates the fundamental rights, and with the other provisions of the Constitution.

Holding that a third ground of challenge – that the law in question is arbitrary – is not available, the decision in **Binoy Viswam** placed reliance on the enunciation of law by a three judge Bench in **State of A P** v **McDowell & Co (Mcdowell)**.[512] **McDowell** ruled that while a challenge to a statute on the ground that it violates the principle of equality under Article 14 is available, a statute cannot be invalidated on the ground that it is arbitrary:

> "43…In other words, say, if an enactment is challenged as violative of Article 14, it can be struck down only if it is found that it is violative of the equality clause/equal protection clause enshrined therein…
> No enactment can be struck down by just saying that it is arbitrary or unreasonable. Some or other constitutional infirmity has to be found before invalidating an Act."[513]

[512] (1996) 3 SCC 709
[513] Ibid, at page 124

In **Binoy Viswam**, the two judge Bench observed that the "contours" of judicial review had been spelt out in **State of Madhya Pradesh** v **Rakesh Kohli**,[514] and more recently in **Rajbala** v **State of Haryana**.[515] Reiterating the same position, **Binoy Viswam** holds:

> "81.Another aspect in this context, which needs to be emphasised, is that a legislation cannot be declared unconstitutional on the ground that it is "arbitrary" inasmuch as examining as to whether a particular Act is arbitrary or not implies a value judgment and the courts do not examine the wisdom of legislative choices and, therefore, cannot undertake this exercise."[516]

274 In the decision of the Constitution Bench in **Shayara Bano** v **Union of India ("Shayara Bano")**,[517] Justice Rohinton Nariman speaking for himself and Justice Uday U Lalit noticed that the dictum in **McDowell,** to the effect that "no enactment can be struck down by just saying it is arbitrary or unreasonable" had failed to notice the judgment of the Constitution Bench in **Ajay Hasia** v **Khalid Mujib Sehravardi ("Ajay Hasia")**,[518] and a three judge Bench decision in **Dr K R Lakshmanan** v **State of T N ("Lakshmanan")**.[519] In **Ajay Hasia,** the Constitution Bench traced the evolution of the doctrine of equality beyond its origins in the doctrine of classification. **Ajay Hasia** ruled that since the decision in **E P Royappa** v **State of Tamil Nadu**,[520] it had been held that equality had a substantive content which, simply put, was the antithesis of arbitrariness. Consequently:

---

[514] (2012) 6 SCC 312
[515] (2016) 2 SCC 445
[516] Ibid, at page 125
[517] (2017) 9 SCC 1
[518] (1981) 1 SCC 722
[519] (1996) 2 SCC 226
[520] (1974) 4 SCC 3

> "16...**Wherever therefore there is arbitrariness in State action whether it be of the legislature or of the executive or of an "authority" under Article 12, Article 14 immediately springs into action and strikes down such State action**. In fact, the concept of reasonableness and non-arbitrariness pervades the entire constitutional scheme and is a golden thread which runs through the whole of the fabric of the Constitution."[521] (Emphasis supplied)

The principle of arbitrariness was applied for invalidating a State law by the three judge Bench decision in **Lakshmanan**. It was, in this context that Justice Nariman speaking for two Judges in the Constitution Bench in **Shayara Bano** held that manifest arbitrariness is a component of Article 14. Hence, a law which is manifestly arbitrary would violate the fundamental right to equality:

> "87. The thread of reasonableness runs through the entire fundamental rights chapter. What is manifestly arbitrary is obviously unreasonable and being contrary to the rule of law, would violate Article 14. Further, there is an apparent contradiction in the three-Judge Bench decision in *McDowe*ll when it is said that a constitutional challenge can succeed on the ground that a law is "disproportionate, excessive or unreasonable", yet such challenge would fail on the very ground of the law being "unreasonable, unnecessary or unwarranted". The arbitrariness doctrine when applied to legislation obviously would not involve the latter challenge but would only involve a law being disproportionate, excessive or otherwise being manifestly unreasonable. All the aforesaid grounds, therefore, do not seek to differentiate between State action in its various forms, all of which are interdicted if they fall foul of the fundamental rights guaranteed to persons and citizens in Part III of the Constitution."[522]

Justice Nariman has observed that even after **McDowell**, challenges to the validity of legislation have been entertained on the ground of arbitrariness

[521] Ajay Hasia at page 741
[522] Ibid, at pages 91-92

(**Malpe Vishwanath Acharya** v **State of Maharashtra**,[523] **Mardia Chemicals Ltd.** v **Union of India**,[524] **State of Tamil Nadu** v **K Shyam Sunder**,[525] **Andhra Pradesh Dairy Development Corporation Federation** v **B Narasimha Reddy**[526] and **K T Plantation Private Limited** v **State of Karnataka**[527]).

275 In **Shayara Bano**, Justice Nariman has adverted to the decisions which have followed **McDowell** including the two judge Bench decision in **Binoy Viswam**. These decisions, in the view of Justice Nariman, are therefore no longer good law:

> "99. However, in State of Bihar v. Bihar Distillery Ltd., SCC at para 22, in State of M.P. v. Rakesh Kohli, SCC at paras 17 to 19, in Rajbala v. State of Haryana, SCC at paras 53 to 65 and in Binoy Viswam v. Union of India, SCC at paras 80 to 82, McDowell was read as being an absolute bar to the use of "arbitrariness" as a tool to strike down legislation under Article 14. As has been noted by us earlier in this judgment, McDowell itself is per incuriam, not having noticed several judgments of Benches of equal or higher strength, its reasoning even otherwise being flawed. The judgments, following McDowell are, therefore, no longer good law."[528]

In the above extract, Justice Nariman has specifically held that the **McDowell** test which barred a challenge to a law on the ground of arbitrariness ignored a binding Constitution Bench view in **Ajay Hasia** and that of a three judge Bench in **Lakshmanan.** Moreover, the above extract from **Shayara Bano**

[523] (1998) 2 SCC 1
[524] (2004) 4 SCC 311
[525] (2011) 8 SCC 737
[526] (2011) 9 SCC 286
[527] (2011) 9 SCC 1
[528] Ibid, at page 97

disapproves of the restriction on judicial review in **Binoy Viswam,** which follows **McDowell**. Justice Kurian Joseph, in the course of his decision has specifically agreed with the view expressed by Justice Nariman:

> "5…However, on the pure question of law that a legislation, be it plenary or subordinate, can be challenged on the ground of arbitrariness, I agree with the illuminating exposition of law by Nariman J. I am also of the strong view that the constitutional democracy of India cannot conceive of a legislation which is arbitrary."

276 In **Puttaswamy,** the judgment delivered on behalf of four Judges expressly recognized the impact of Article 14 in determining whether a law which is challenged on the ground that it violates Article 21 meets both the procedural as well as the substantive content of reasonableness. The Court held:

> "291… the evolution of Article 21, since the decision in Cooper indicates two major areas of change. First, the fundamental rights are no longer regarded as isolated silos or watertight compartments. In consequence, Article 14 has been held to animate the content of Article 21. Second, the expression "procedure established by law" in Article 21 does not connote a formalistic requirement of a mere presence of procedure in enacted law. That expression has been held to signify the content of the procedure and its quality which must be fair, just and reasonable. The mere fact that the law provides for the deprivation of life or personal liberty is not sufficient to conclude its validity and the procedure to be constitutionally valid must be fair, just and reasonable. The quality of reasonableness does not attach only to the content of the procedure which the law prescribes with reference to Article 21 but to the content of the law itself. In other words, the requirement of Article 21 is not fulfilled only by the enactment of fair and reasonable procedure under the law and a law which does so may yet be susceptible to challenge on the ground that its content does not accord with the requirements of a valid law. The law is open to substantive challenge on the ground that it violates the fundamental right."[529]

[529] Ibid, at page 495

The same principle has been emphasized in the following observations:

> "294…Article 14, as a guarantee against arbitrariness, infuses the entirety of Article 21. The interrelationship between the guarantee against arbitrariness and the protection of life and personal liberty operates in a multi-faceted plane. First, it ensures that the procedure for deprivation must be fair, just and reasonable. Second, Article 14 impacts both the procedure and the expression "law". A law within the meaning of Article 21 must be consistent with the norms of fairness which originate in Article 14. As a matter of principle, once Article 14 has a connect with Article 21, norms of fairness and reasonableness would apply not only to the procedure but to the law as well."[530]

277 In **Binoy Viswam**, the two judge Bench held that while enrolment under the Aadhaar Act is voluntary, it was legitimately open to the Parliament, while enacting Section 139AA of the Income Tax Act to make the seeding of the Aadhaar number with the PAN card mandatory. The court held that the purpose of making it mandatory under the Income Tax Act was to curb black money, money laundering and tax evasion. It was open to Parliament to do so and its legislative competence could not be questioned on that ground. The court held that the legislative purpose of unearthing black money and curbing money laundering furnished a valid nexus with the objective sought to be achieved by the law:

> "105. Unearthing black money or checking money laundering is to be achieved to whatever extent possible. Various measures can be taken in this behalf. If one of the measures is introduction of Aadhaar into the tax regime, it cannot be denounced only because of the reason that the purpose would not be achieved fully. Such kind of menace, which is deep-rooted, needs to be tackled by taking multiple actions and those actions may be initiated at the same time. It is the combined effect of these actions which may yield results and

[530] Ibid, at page 496

> each individual action considered in isolation may not be sufficient. Therefore, rationality of a particular measure cannot be challenged on the ground that it has no nexus with the objective to be achieved. Of course, there is a definite objective. For this purpose alone, individual measure cannot be ridiculed. We have already taken note of the recommendations of SIT on black money headed by Justice M.B. Shah. We have also reproduced the measures suggested by the Committee headed by Chairman, CBDT on "Measures to Tackle Black Money in India and Abroad". They have, in no uncertain terms, suggested that one singular proof of identity of a person for entering into finance/business transactions, etc. may go a long way in curbing this foul practice. That apart, even if solitary purpose of de-duplication of PAN cards is taken into consideration, that may be sufficient to meet the second test of Article 14. It has come on record that 11.35 lakh cases of duplicate PAN or fraudulent PAN cards have already been detected and out of this 10.52 lakh cases pertain to individual assessees. Seeding of Aadhaar with PAN has certain benefits which have already been enumerated. Furthermore, even when we address the issue of shell companies, fact remains that companies are after all floated by individuals and these individuals have to produce documents to show their identity. It was sought to be argued that persons found with duplicate/bogus PAN cards are hardly 0.4% and, therefore, there was no need to have such a provision. We cannot go by percentage figures. The absolute number of such cases is 10.52 lakhs, which figure, by no means, can be termed as miniscule, to harm the economy and create adverse effect on the nation. The respondents have argued that Aadhaar will ensure that there is no duplication of identity as biometrics will not allow that and, therefore, it may check the growth of shell companies as well.
>
> 106. Having regard to the aforesaid factors, it cannot be said that there is no nexus with the objective sought to be achieved."[531]

The court observed that it was a harsh reality of our times that the benefit of welfare measures adopted by the State does not reach the segments of society for whom they are intended:

> "125.1.3… However, for various reasons including corruption, actual benefit does not reach those who are supposed to receive such benefits. One of the main reasons is failure to

[531] Ibid, at pages 134-135

> identify these persons for lack of means by which identity could be established of such genuine needy class. Resultantly, lots of ghosts and duplicate beneficiaries are able to take undue and impermissible benefits. A former Prime Minister of this country has gone on record to say that out of one rupee spent by the Government for welfare of the downtrodden, only 15 paisa thereof actually reaches those persons for whom it is meant. It cannot be doubted that with UID/Aadhaar much of the malaise in this field can be taken care of."[532]

In this context, the court also noted that as a result of de-duplication exercises, 11.35 lakh cases of duplicate PANs / fraudulent PANs had been detected out of which 10.52 lakh cases pertained to individual assesses. The court upheld the decision of Parliament as the legislating body of seeding PANs with Aadhaar as "the best method, and the only robust method of de-duplication of PAN database".

278 The edifice of Section 139AA is based on the structure created by the Aadhaar Act. Section 139AA of the Income Tax Act 1962 is postulated on the requirement of Aadhaar having been enacted under a valid piece of legislation. The validity of the legislation seeding Aadhaar to PAN is dependent upon and cannot be segregated from the validity of the parent Aadhaar legislation. In fact, that is one of the reasons why in **Binoy Viswam,** the Article 21 challenge was not adjudicated upon since that was pending consideration before a larger Bench. The validity of seeding Aadhaar to PAN under Section 139AA must therefore depend upon the constitutional validity of the Aadhaar Act as it is determined by this Court. Further Rule 114B of the

[532] Ibid, at page 146

Income Tax Rules 1962 provides for a list of transactions for which a person must quote a PAN card number. Rule 114B requires that a person must possess a PAN card for those transactions. These are summarized below:

- "Sale or purchase of a motor vehicle or vehicle, as defined in clause (28) of section 2 of the Motor Vehicles Act, 1988 (59 of 1988) which requires registration by a registering authority under Chapter IV of that Act, other than two wheeled vehicles.
- Opening an account [other than a time-deposit and a Basic Savings Bank Deposit Account] with a banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949), applies (including any bank or banking institution referred to in section 51 of that Act).
- Making an application to any banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949), applies (including any bank or banking institution referred to in section 51 of that Act) or to any other company or institution, for issue of a credit or debit card.
- Opening of a demat account with a depository, participant, custodian of securities or any other person registered under sub-section (1A) of section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992).
- Payment to a hotel or restaurant against a bill or bills at any one time.
- Payment in connection with travel to any foreign country or payment for purchase of any foreign currency at any one time.
- Payment to a Mutual Fund for purchase of its units.
- Payment to a company or an institution for acquiring debentures or bonds issued by it.
- Payment to the Reserve Bank of India, constituted under section 3 of the Reserve Bank of India Act, 1934 (2 of 1934) for acquiring bonds issued by it.
- Deposit with,—
    - banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949), applies (including any bank or banking institution referred to in section 51 of that Act);
    - Post Office.
- Purchase of bank drafts or pay orders or banker's cheques from a banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949),

applies (including any bank or banking institution referred to in section 51 of that Act).

- A time deposit with, —
  - a banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949), applies (including any bank or banking institution referred to in section 51 of that Act);
  - a Post Office;
  - a Nidhi referred to in section 406 of the Companies Act, 2013 (18 of 2013); or
  - a non-banking financial company which holds a certificate of registration under section 45-IA of the Reserve Bank of India Act, 1934 (2 of 1934), to hold or accept deposit from public.
- Payment for one or more pre-paid payment instruments, as defined in the policy guidelines for issuance and operation of pre-paid payment instruments issued by Reserve Bank of India under section 18 of the Payment and Settlement Systems Act, 2007 (51 of 2007), to a banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949), applies (including any bank or banking institution referred to in section 51 of that Act) or to any other company or institution.
- Payment as life insurance premium to an insurer as defined in clause (9) of section 2 of the Insurance Act, 1938 (4 of 1938).
- A contract for sale or purchase of securities (other than shares) as defined in clause (h) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956).
- Sale or purchase, by any person, of shares of a company not listed in a recognised stock exchange.
- Sale or purchase of any immovable property.
- Sale or purchase, by any person, of goods or services of any nature other than those specified above."

The decision in **Puttaswamy** has recognised that protection of the interests of the revenue constitutes a legitimate state aim in the three-pronged test of proportionality. The circumstances which have been adverted to in the decision in **Binoy Viswam** are a sufficient indicator of the legitimate concerns of the revenue to curb tax evasion, by embarking upon a programme for de-duplication of the Pan data base. A legitimate state aim does exist. However,

that in itself is not sufficient to uphold the validity of the law, which must meet the other parameters of proportionality spelt out in **Puttaswamy.** The explanation to Section 139AA adopts the definition of the expressions 'Aadhaar number', 'enrolment' and 'resident' from the parent Aadhaar legislation. The seeding of Aadhaar with Pan cards must depend for its validity on the constitutional validity of the Aadhaar legislation. Hence, besides affirming that the object of the measure in Section 139AA constitutes a legitimate state aim, the decision of this Court in regard to the validity of Aadhaar will impact upon the seeding of PAN with Aadhaar, which Section 139AA seeks to achieve.

H.7 Linking of SIM cards and Aadhaar numbers

279 In **Avishek Goenka** v **Union of India**[533], a three judge Bench of this Court dealt with a public interest litigation seeking to highlight the non-observance of norms, regulations and guidelines relating to subscriber verification by Telecom Service Providers (TSPs). The Department of Telecommunications (DoT), in the course of the proceedings, filed its instructions stating its position in regard to the verification of prepaid and postpaid mobile subscribers. While concluding the proceedings, this Court directed the constitution of an expert committee comprising of representatives of TRAI and DoT. The court mandated that the following issues should be examined by the Committee:

[533] (2012) 5 SCC 275

> "(*a*) Whether re-verification should be undertaken by the service provider/licensee, DoT itself or any other central body?
>
> (*b*) Is there any need for enhancing the penalty for violating the instructions/guidelines including sale of pre-activated SIM cards?
>
> (*c*) Whether delivery of SIM cards may be made by post? Which is the best mode of delivery of SIM cards to provide due verification of identity and address of a subscriber?
>
> (*d*) Which of the application forms i.e. the existing one or the one now suggested by TRAI should be adopted as universal application form for purchase of a SIM card?
>
> (*e*) In absence of Unique ID card, whether updating of subscriber details should be the burden of the licensee personally or could it be permitted to be carried out through an authorised representative of the licensee?
>
> (*f*) In the interest of national security and the public interest, whether the database of all registered subscribers should be maintained by DoT or by the licensee and how soon the same may be made accessible to the security agencies in accordance with law?"[534]

In pursuance of the above directive, DoT issued instructions on the verification of new mobile subscribers on 9 August 2012. On 6 January 2016, TRAI addressed a communication to DoT recommending that the new procedure for subscriber verification was "cumbersome and resource intensive" and hence should be replaced by an Aadhaar linked e-KYC mechanism. Following this, DoT issued a directive on 16 August 2016 to launch an Aadhaar e-KYC service across all licenced service areas for issuance of mobile connections. However, it was stated that the e-KYC process was an alternative, in addition to the existing process of issuing mobile connections to subscribers and would not be applicable for bulk, outstation and foreign customers.

[534] Ibid, at page 283

280 A public interest litigation was filed before this Court under Article 32 in **Lokniti Foundation** v **Union of India**[535]. The relief which claimed was that there should be a definite mobile phone subscriber verification to ensure a hundred per cent verification of subscribers. Responding to the petition, the Union Government informed this Court that DoT had launched an Aadhaar based e-KYC for issuing mobile connections on 16 August 2016, by which customers as well as point of sale agents of TSPs will be authenticated by UIDAI. A statement was made by the learned Attorney General that an effective programme for verification of prepaid connections would be devised within one year. In view of the statement of the AG, the petition was disposed of by a two judge Bench in terms of the following directions:

> "5. In view of the factual position brought to our notice during the course of hearing, we are satisfied, that the prayers made in the writ petition have been substantially dealt with, and an effective process has been evolved to ensure identity verification, as well as, the addresses of all mobile phone subscribers for new subscribers. In the near future, and more particularly, within one year from today, a similar verification will be completed, in the case of existing subscribers. While complimenting the petitioner for filing the instant petition, we dispose of the same with the hope and expectation, that the undertaking given to this Court, will be taken seriously, and will be given effect to, as soon as possible."[536]

Following the decision, DoT issued a directive on 23 March 2017 to all licensees stating that a way forward had been found to implement the directions of the Supreme Court. Based on the hypothesis that this Court had directed an E-KYC verification, DoT proceeded to implement it on 23 March 2017.

[535] (2017) 7 SCC 155
[536] Ibid, at page 156

281 Mr Rakesh Dwivedi, learned Senior Counsel appearing on behalf of UIDAI and the State of Gujarat supported the measure. He submitted that the licences of all TSPs are issued under Section 4 of the Indian Telegraph Act 1885. Since the Central Government has the exclusive privilege of establishing, maintaining and working telegraphs, TSPs, it was urged, have to operate the telegraph under a license and the Central Government is entitled to impose conditions on the licensee. The instruction issued by DoT on 23 March 2017 has, it is urged, the sanction of Section 4 of the Indian Telegraph Act 1885.

282 We must at the outset note the ambit of the proceedings before this Court in **Lokniti Foundation.** In response to the public interest litigation, it was the Union Government which relied on its decision of 16 August 2016 to implement e-KYC verification for mobile subscribers. The petition was disposed of since the prayers were substantially dealt with and the court perceived that an effective process had been adopted to ensure identity verification together with verification of addresses. Existing subscribers were directed to be verified in a similar manner within one year. The issue as to whether the seeding of Aadhaar with mobile SIM cards was constitutionally valid did not fall for consideration.

283 The decision to link Aadhaar numbers with SIM cards and to require e-KYC authentication of mobile subscribers has been looked upon by the Union

government purely as a matter of efficiency of identification. TRAI's letter dated 6 January 2016 states that the new procedure for subscriber verification which it had adopted was "cumbersome and resource intensive". The issue as to whether Aadhaar linked e-KYC authentication would seriously compromise the privacy of mobile subscribers did not enter into the decision making calculus. In applying the test of proportionality, the matter has to be addressed not just by determining as to 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.

284 The submission that a direction of this nature could have been given to TSPs under Section 4 of the Indian Telegraph Act 1885 does not answer the basic issue of its constitutional validity, which turns upon the proportionality of the measure. Having due regard to the test of proportionality which has been propounded in **Puttaswamy** and as elaborated in this judgment, we do not find that the decision to link Aadhaar numbers with mobile SIM cards is valid or constitutional. The mere existence of a legitimate state aim will not justify the means which are adopted. Ends do not justify means, at least as a matter of constitutional principle. For the means to be valid, they must be carefully tailored to achieve a legitimate state aim and should not be either disproportionate or excessive in their encroachment on individual liberties.

285 Mobile technology has become a ubiquitous feature of our age. Mobile phones are not just instruments to facilitate a telephone conversation. They are a storehouse of data reflecting upon personal preferences, lifestyles and individual choices. They bear upon family life, the workplace and personal intimacies. The conflation of biometric data with SIM cards is replete with grave dangers to personal autonomy. A constitution based on liberal values cannot countenance an encroachment of this nature. The decision to link Aadhaar numbers to SIM cards and to enforce a regime of e-KYC authentication clearly does not pass constitutional muster and must stand invalidated. All TSPs shall be directed by the Union government and by TRAI to forthwith delete the biometric data and Aadhaar details of all subscribers

within two weeks. The above data and Aadhaar details shall not be used or purveyed by any TSP or any other person or agency on their behalf for any purpose whatsoever.

I Money laundering rules

286 Parliament enacted a law on money-laundering as part of a concerted effort by the international community to deal with activities which constitute a threat to financial systems and to the integrity and sovereignty of nations. The Statement of Objects and Reasons accompanying the introduction of the Bill contains an elucidation of the reasons for the enactment:

> "**Introduction**
> Money-laundering poses a serious threat not only to the financial systems of countries, but also to their integrity and sovereignty. To obviate such threats international community has taken some initiatives. It has been felt that to prevent money-laundering and connected activities a comprehensive legislation is urgently needed. To achieve this objective the Prevention of Money-laundering Bill, 1998 was introduced in the Parliament. The Bill was referred to the Standing Committee on Finance, which presented its report on 4th March 1999 to the Lok Sabha. The Central Government broadly accepted the recommendation of the Standing Committee and incorporated them in the said Bill along with some other desired changes.
>
> **Statement of Objects and Reasons**
> It is being realized, world over, that money-laundering poses a serious threat not only to the financial systems of countries, but also to their integrity and sovereignty. Some of the initiatives taken by the international community to obviate such threat are outlined below:-
> (a) the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, to which India is a party, calls for prevention of laundering of proceeds of drug crimes and other connected activities and confiscation of proceeds derived from such offence.
> (b) the Basle Statement of Principles, enunciated in 1989, outlined basic policies and procedures that banks should

follow in order to assist the law enforcement agencies in tackling the problem of money laundering.

(c) the Financial Action Task Force established at the summit of seven major industrial nations, held in Paris from 14th to 16th July 1989, to examine the problem of money-laundering has made forty recommendations, which provide the foundation material for comprehensive legislation to combat the problem of money-laundering. The recommendations were classified under various heads. Some of the important heads are-

(i) declaration of laundering of monies carried through serious crimes a criminal offence;

(ii) to work out modalities of disclosure by financial institutions regarding reportable transactions;

(iii) confiscation of the proceeds of crime;

(iv) declaring money-laundering to be an extraditable offence; and

(v) promoting international co-operation in investigation of money-laundering.

(d) the Political Declaration and Global Programme of Action adopted by United Nations General Assembly by its Resolution No. S-17/2 of 23rd February 1990, *inter alia,* calls upon the member States to develop mechanism to prevent financial institutions from being used for laundering of drug related money and enactment of legislation to prevent such laundering.

(e) the United Nations in the Special Session on countering World Drug Problem Together concluded on the 8th to the 10th June 1998 has made another declaration regarding the need to combat money-laundering. India is a signatory to this declaration."

287 The expressions "beneficial owner, reporting entity and intermediary" are defined respectively in clauses (fa), (wa) and (n) of the Act thus:

"(fa) "beneficial owner" means an individual who ultimately owns or controls a client of a reporting entity or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person.

(wa) "reporting entity" means a banking company, financial institution, intermediary or a person carrying on a designated business or profession.

(n) "intermediary" means,-

(i) a stock-broker, sub-broker share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue,

> merchant banker, underwriter, portfolio manager, investment adviser or any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992); or
> (ii) an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 (74 of 1952) or any member of such association; or
> (iii) intermediary registered by the Pension Fund Regulatory and Development Authority; or
> (iv) a recognised stock exchange referred to in clause (f) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956)."

The Prevention of Money-Laundering (Maintenance of Records) Rules 2005 were amended by the Prevention of Money-Laundering (Maintenance of Records) Second Amendment Rules 2017. By the amendment, several definitions were introduced with reference to the provisions of the Aadhaar Act. These are:

> "'(aaa) "Aadhaar number" means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
> (aab) "authentication" means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
> (aac) "Resident" means an individual as defined under sub-section (v) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
> (aad) "identity information" means the information as defined in sub-section (n) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
> (aae) "e – KYC authentication facility" means an authentication facility as defined in Aadhaar (Authentication) Regulations, 2016;
> (aaf) "Yes/No authentication facility" means an authentication facility as defined in Aadhaar (Authentication) Regulations, 2016…"

Similarly, the expression "officially valid document" was amended to read as follows:

> "(d) **"officially valid document"** means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by [Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and **Aadhaar number or any other document as notified by the Central Government in consultation with the [Regulator]:**
> [Provided that where simplified measures are applied for verifying the identity of the clients the following documents shall be deemed to be officially valid documents:-
> (a) identity card with applicant's Photograph issued by the Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks and Public Financial Institutions;
> (b) letter issued by a gazette officer, with a duly attested photograph of the person]."

288 Rule 9 of the 2005 Rules requires every reporting entity to carry out client due diligence at the time of the commencement of an account-based relationship. Due diligence requires a verification of the identity of the client and a determination of whether the client is acting on behalf of a beneficial owner, who then has to be identified. Rule 9(3) defines the expression "beneficial owner" for the purpose of sub-rule 1. Rule 9(4) requires an individual client to submit an Aadhaar number. Rule 9(3) and Rule 9(4) are extracted below:

> "9. Client Due Diligence.—(1) Every reporting entity shall—
> xxxxx
> xxxxx
> (3) The beneficial owner for the purpose of sub-rule (1) shall be determined as under—
> (a) where the client is a company, **the beneficial owner is the natural person(s),** who, whether acting alone or

together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation.—For the purpose of this sub-clause-

1. **"Controlling ownership interest"** means ownership of or entitlement to more than twenty-five per cent. of shares or capital or profits of the company;

2. **"Control" shall include the right to appoint majority of the directors or to control the management or policy** decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

(b) where the client is **a partnership firm,** the beneficial owner is the natural person(s) who, whether acting alone or \ together, or through one or more juridical person, has I ownership of/ entitlement to more than fifteen per cent. of capital or profits of the partnership;

(c) where the client is **an unincorporated association** or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of such association or body of individuals;

(d) where no natural person is identified under (a) or (b) or (c) above, **the beneficial owner is the relevant natural person who holds the position of senior managing official**;

(e) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

(f) **where the client or the owner of the controlling interest is a company listed on a stock exchange,** or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(4) **Where the client is an individual, who is eligible to be enrolled for an Aadhaar number,** he shall for the purpose of sub-rule (1) submit to the reporting entity, -

(a) **the Aadhaar number issued by the Unique Identification Authority of India;** and

(b) **the Permanent Account Number** or **Form No. 60** as defined in Income-tax Rules, 1962, and such other documents including in respect of the nature of business and financial status of the client as may be required by the reporting entity:

Provided that where an Aadhaar number has not been assigned to a client, the client shall furnish proof of application of enrolment for Aadhaar and in case the

> Permanent Account Number is not submitted, one certified copy of an 'officially valid document' shall be submitted.
> Provided further that photograph need not be submitted by a client falling under clause (b) of sub-rule (1)."
> (Emphasis supplied)

Sub-rule 15 of Rule 9 requires the reporting entity to carry out authentication at the time of receipt of the Aadhaar number:

> "(15) Any reporting entity, at the time of receipt of the Aadhaar number under provisions of this rule, shall carry out authentication using either e-KYC authentication facility or Yes/No authentication facility provided by Unique Identification Authority of India."

Sub-rule 17 allows a period of six months for a client who is eligible to be enrolled for Aadhaar and to obtain a PAN to submit it upon the commencement of the account-based relationship. Failure to do so, would result in the account ceasing to be operational until the Aadhaar number and PAN are submitted. Clauses a and c of sub-rule 17 provide as follows :

> "(17) (a) In case the client, eligible to be enrolled for Aadhaar and obtain a Permanent Account Number, referred to in sub-rules (4) to (9) of rule 9 does not submit the Aadhaar number or the Permanent Account Number at the time of commencement of an account based relationship with a reporting entity, the client shall submit the same within a period of six months from the date of the commencement of the account based relationship:
> Provided that the clients, eligible to be enrolled for Aadhaar and obtain the Permanent Account Number, already having an account based relationship with reporting entities prior to date of this notification, the client shall submit the Aadhaar number and Permanent Account Number by 31st December, 2017.
> (c) In case the client fails to submit the Aadhaar number and Permanent Account Number within the aforesaid six months period, the said account shall cease to be operational till the time the Aadhaar number and Permanent Account Number is submitted by the client:

Provided that in case client already having an account based relationship with reporting entities prior to date of this notification fails to submit the Aadhaar number and Permanent Account Number by 31st December, 2017, the said account shall cease to be operational till the time the Aadhaar number and Permanent Account Number is submitted by the client."

289 The statutory mandate for the framing these rules is contained in Sections 12, 15 and 73 of the PMLA. Insofar as is material, Section 12 provides as follows:

"12. Reporting entity to maintain records:-

(1) Every reporting entity shall-

(a) maintain a record of all transactions, including information relating to transactions covered under clause (b), in such manner as to enable it to reconstruct individual transactions;

(b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;

(c) **verify the identity of its clients in such manner and <u>subject to such conditions,</u> as may be prescribed;**

(d) **identify the beneficial owner, if any, of such of its clients, as may be prescribed;**

(e) **maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.**

(2) Every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.

(3) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

(4) The records referred to in clause (e) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been close, whichever is later.

(5) The Central Government may, by notification, exempt any reporting entity or class of reporting entities from any obligation under this Chapter."

(Emphasis supplied)

Section 12 imposes a statutory obligation on reporting entities to maintain records and to verify the identity of their clients and beneficial owners in the manner prescribed. The procedure for and manner in which information is furnished by reporting entities is specified under sub-section 1 of Section 12 by the Central Government in consultation with the Reserve Bank of India. Section 15 provides as follows:

> "15. Procedure and manner of furnishing information by reporting entities:-
> The Central Government may, in consultation with the Reserve Bank of India, prescribe the procedure and the manner of maintaining and furnishing information by a reporting entity under sub-section (1) of Section 12 **for the purpose of implementing the provisions of this Act**."
> (Emphasis supplied)

The rule making power is referable to the provisions of Section 73, which insofar as is material, provides as follows:

> "73. Power to make rules-
> (1) The Central Government may, by notification, make rules for carrying out the provisos of this Act.
> (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely-
>
> (j) the manner and the conditions in which identity of clients shall be verified by the reporting entities under clause (c) of sub-section (1) of Section 12;
> (jj) the manner of identifying beneficial owner, if any, from the clients by the reporting entities under clause (d) of sub-section (1) of Section 12;
> (k) the procedure and the manner of maintaining and furnishing information under sub-section (1) of Section 12 as required under Section 15;
> (x) any other matter which is required to be, or may be, prescribed."

Section 12(1)(c) requires the reporting entity to verify the identity of its clients "in such manner and subject to such conditions" as may be prescribed. The

provisions of the rules, including sub-rule 17(c) of Rule 9 have been challenged on the ground that they suffer from the vice of excessive delegation.

290 In **Bombay Dyeing and Mfg** v **Bombay Environmental Action Group**[537], this Court has re-affirmed the well-settled legal test which determines the validity of delegated legislation. The court held:

> "104**…**By reason of any legislation, whether enacted by the legislature or by way of subordinate legislation, the State gives effect to its legislative policy. Such legislation, however, must not be ultra vires the Constitution. A subordinate legislation apart from being intra vires the Constitution, should not also be ultra vires the parent Act under which it has been made. A subordinate legislation, it is trite, must be reasonable and in consonance with the legislative policy as also give effect to the purport and object of the Act and in good faith."

The essential legislative function consists in the determination of legislative policy and of formally enacting it into a binding rule of conduct. Once this is carried out by the legislature, ancillary or subordinate functions can be delegated. Having laid down legislative policy, the legislation may confer discretion on the executive to work out the details in the exercise of the rule making power, though, in a manner consistent with the plenary enactment (**J K Industries Ltd** v **Union of India**[538]).

291 The Reserve Bank of India had issued a Master Circular dated 25 February 2016 in exercise of its statutory powers under Section 35A of the

[537] (2006) 3 SCC 434
[538] (2007) 13 SCC 673

Banking Regulation Act 1949 (read with Section 56) and Rule 9(14) of the Prevention of Money-Laundering (Maintenance of Records) Rules 2005. Following the amendment of the PMLA Rules, the Master Circular of the Reserve Bank has been updated on 20 April 2018.

The basic issue which needs to be addressed is whether the amendments which were brought about to the PMLA Rules in 2017 meet the test of proportionality.

292 In 2005, the Central Government in consultation with the Reserve Bank of India notified the Prevention of Money-Laundering (Maintenance of Records) Rules 2005 under Section 73 of the parent Act. The expression 'officially valid document' was defined in Rule 2(d) in the following terms :

> "(d) "officially valid document" means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by[539] [Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India[540] [or the National Population Register] containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the [Regulator];"

Rule 9(4) required the submission to the reporting entity, where the client is an individual, a certified copy of an officially valid document containing details of identity and address. Rule 9(4) read as follows :

> "(4) Where the client is an individual, he shall for the purpose of sub-rule (1), submit to the reporting entity, one certified

[539] Substituted by G.S.R. 980(E), dated 16-12-2010 (w.e.f. 16-12-2010)
[540] Inserted by G.S.R. 544(E)

> copy of an "officially valid document" containing details of his identity and address, one recent photograph and such other documents including in respect of the nature of business and financial status of the client as may be required by the reporting entity:"

Under Rule 9(14), the regulator was empowered to issue guidelines, in terms of the provisions of the rule, and to prescribe enhanced or simplified measures to verify the identity of a client, taking into consideration the type of client, business relationship, and the nature and value of transactions based on the overall money-laundering and terrorist financing risks involved. Under the above rules there were six 'officially valid documents' : the passport, driving licence, Permanent Account Number (PAN) Card, NREGA job card, Voter's Identity Card and a letter of UIDAI containing details of name, address and details of Aadhaar number. or any other document notified by the Central Government in consultation with the Regulator.

293 In the Master Circular issued by the Reserve Bank of India on 25 February 2016, a provision was made for the submission by customers, at their option, of one of the six officially valid documents (OVDs) for proof of identity and address. Rule 3(vi) defined the expression 'officially valid document' in similar terms:

> "(vi) "officially valid document" means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

> Explanation: Customers, at their option, shall submit one of the six OVDs for proof of identity and proof of address."

Customer due diligence and on-going due diligence were defined thus:

> "Customer Due Diligence (CDD)" means indemnifying and verifying the customer and the beneficial owner using 'Officially Valid Documents' as a 'proof of identity' and a 'proof of address'.
> "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds."

294 Chapter III of the Master Circular provided for regulated entities (including banks) to specify a customer acceptance policy. Clause 15 of the Master Circular *inter alia* specified that customers shall not be required to furnish additional OVDs if the OVD already submitted, contained both proof of identity and address. Chapter VI which provided for a due diligence procedure allowed customers to submit one of the six OVDs for proof of identity and address. Under Part V of Chapter VI, banks were required to conduct on-going due diligence particularly in regard to large and complex transactions above a threshold. Clause 39 of the Circular provided for a partial freezing and closure of accounts:

> "39. **Partial freezing and closure of accounts**
> (a) Where REs are unable to comply with the CDD requirements mentioned at Part I to V above, they shall not open accounts, commence business relations or perform transactions. In case of existing business relationship which is not KYC compliant, banks shall ordinarily take step to terminate the existing business relationship after giving due notice.
> (b) As an exception to the Rule, banks shall have an option to choose not to terminate business relationship straight away and instead opt for a phased closure of operations in this account as explained below:

i. The option of 'partial freezing' shall be exercise after giving due notice of three months to the customers to comply with KYC requirements.
ii. A reminder giving a further period of three months shall also be given.
iii. Thereafter, 'partial freezing' shall be imposed by allowing credits and disallowing all debits with the freedom to close the accounts in case of the account being KYC non-compliant after six months of issue first notice.
iv. All debits and credits from/to the accounts shall be disallowed, in case of the account being KYC non-compliant after six months of imposing 'partial freezing',
v. The account holders shall have the option, to revive their accounts by submitting the KYC documents.

(c) When an account is closed whether without 'partial freezing' or after 'partial freezing', the reason for that shall be communicated to account holder."

Chapter VIII provided for reporting requirements to the Financial Intelligence Unit. Chapter IX dealt with compliance with requirements/obligations under international agreements. Clause 58 of Chapter X stipulated reporting requirements under the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS).

295 As a result of the amendment to the Rules brought about in 2017, Rule 9(4) mandates that in the case of a client who is an individual, who is eligible to be enrolled for an Aadhaar number, submission of the Aadhaar number is mandatory. Instead of furnishing an option to submit one of six OVDs, submission of Aadhaar number alone is mandated. Where an Aadhaar number has not been assigned, proof of an application for enrolment is required to be submitted. Under Rule 9(15), the reporting entity at the time of

receipt of an Aadhaar number is under an obligation to carry out authentication using either the e-KYC authentication facility or the yes/no authentication provided by UIDAI. If a client who is eligible to be enrolled for Aadhaar and to obtain a PAN card does not submit its details while commencing an account based relationship, there is a period of six months reserved for submission. Those who already have accounts are required to submit their Aadhaar numbers by a stipulated date. Failure to do so, renders the account subject to the consequence that it shall cease to be operational until compliance is effected.

Following the amendments to the rules, the Reserve Bank has updated its Master Circular on 20 April 2018 to bring it into conformity with the amended rules.

296 In deciding whether the amendment brought about in 2017 to the rules is valid, it is necessary to bear in mind what has already been set out earlier on the aspect of proportionality. Does the requirement of the submission or linking of an Aadhaar number to every account- based relationship satisfy the test of proportionality?

The state has a legitimate aim in preventing money-laundering. In fact, it is with a view to curb and deal with money-laundering that the original version of the Master Circular as well as its updated version impose conditions for initial

and on-going due diligence. The Reserve Bank has introduced several reporting requirements including those required to comply with FATCA norms. The existence of a legitimate state aim satisfies only one element of proportionality. In its submissions, the Union government has dealt only with legitimate aim, leaving the other elements of proportionality unanswered. Requiring every client in an account based relationship to link the Aadhaar number with a bank account and to impose an authentication requirement, is excessive to the aim and object of the state. There can be no presumption that all existing account holders as well as every individual who seeks to open an account in future is a likely money-launderer. The type of client, the nature of the business relationship, the nature and value of the transactions and the terrorism and laundering risks involved may furnish a basis for distinguishing between cases and clients. The rules also fail to make a distinction between opening an account and operating an account. If an account has been opened in the past, it would be on the basis of an established identity. The consequences of the non-submission of an Aadhaar number are draconian. Non-submission within the stipulated period will result in a consequence of the account ceasing to be operational. A perfectly genuine customer who is involved in no wrongdoing would be deprived of the use of the moneys and investments reflected in the account, in violation of Article 300A of the Constitution purely on an assumption that he or she has indulged in money-laundering. The classification is over-inclusive: a uniform requirement of such a nature cannot be imposed on every account based relationship irrespective

of the risks involved to the financial system. The account of a pensioner or of a salaried wage earner cannot be termed with the same brush as a high net-worth individual with cross-border inflows and outflows. Treating every account holder with a highly intrusive norm suffers from manifest arbitrariness. Moreover, there is no specific provision in the Act warranting a consequence of an account holder being deprived of the moneys standing in the account, even if for a temporary period. Section 12(1)(c) empowers a reporting entity to verify the entity or its client in such a manner and "subject to such conditions" as may be prescribed. This does not envisage a consequence of an account ceasing to be operational. Blocking an account is a deprivation of property under Article 300A. The Union Government has been unable to discharge the burden of establishing that this was the least intrusive means of achieving its aim to prevent money-laundering or that its object would have been defeated if it were not to impose the requirement of a compulsory linking of Aadhaar numbers with all account based relationships with the reporting entity. Money-laundering is indeed a serious matter and the Union Government is entitled to take necessary steps including by classifying transactions and sources which give rise to reasonable grounds for suspecting a violation of law. But, to impose a uniform requirement of linking Aadhaar numbers with all account based relationships is clearly disproportionate and excessive. It fails to meet the test of proportionality and suffers from manifest arbitrariness. While we have come to the above conclusion, we clarify that this would not preclude the Union Government in the exercise of its rule making

power and the Reserve Bank of India as the regulator to re-design the requirements in a manner that would ensure due fulfillment of the object of preventing money-laundering, subject to compliance with the principles of proportionality as outlined in this judgment.

J Savings in Section 59

297 Section 59 of the Aadhaar Act provides:

> "Anything done or any action taken by the Central Government under the Resolution of the Government of India, Planning Commission bearing notification number A-43011/02/2009-Admin. I, dated the 28th January, 2009, or by the Department of Electronics and Information Technology under the Cabinet Secretariat Notification bearing notification number S.O. 2492(E), dated the 12th September, 2015, as the case may be, shall be deemed to have been validly done or taken under this Act."

298 The petitioners have submitted that all acts done pursuant to the Notifications dated 28 January 2009 and 12 September 2015, under which the Aadhaar programme was created and implemented, violate fundamental rights and were not supported by the authority of law. It has been submitted that the collection, storage and use of personal data by the State and private entities, which was done in a legislative vacuum as the State failed to enact the Aadhaar Act for six years, is now being sought to be validated by Section 59. It has been contended that since the acts done prior to the enactment of the Aadhaar Act are in breach of fundamental rights, Section 59 is invalid. Moreover, Section 59 does not operate to validate the collection of biometric data prior to the enforcement of the Aadhaar Act.

It has been submitted that a validating law must remove the cause of invalidity of previous acts: it would not be effective if it simply deems a legal consequence without amending the law from which the consequence could follow. In the present case, it has been contended, Section 59 does not create a legal fiction where the Aadhaar Act is deemed to have been in existence since 2009 and that it only declares a legal consequence of the acts done by the Union since 2009.

It has also been submitted that Section 59 is invalid and unconstitutional inasmuch as for Aadhaar enrolments done before 2016, there was neither informed consent nor were any procedural guarantees and safeguards provided under a legal framework. Section 59, it is contended, cannot cure the absence of consent and other procedural safeguards, provided under the Aadhaar Act, to the enrolments done prior to the enactment of the Act.

299 The respondents have submitted that Section 59 protects the actions taken by the Central government. It does not contemplate the maintenance of any data base, containing identity information, by the State governments. The State governments, it is urged, have destroyed the biometric data collected during Aadhaar enrolments before the Act came into force, from their server. It has been contended that Section 59 is retrospective in nature as it states that it shall operate from an earlier date.

The Respondents have relied upon the judgments of this Court in **West Ramnad Electric Distribution Co. Ltd.** v **State of Madras**[541] **("West Ramnad")**, **State of Mysore** v **D. Achiah Chetty, Etc**[542] **("Chetty")**, and **Hari Singh** v **Military Estate Officer**[543] **("Hari Singh")** to contend that the legislature can, by retrospective operation, cure the invalidity of actions taken under a law which is void for violating fundamental rights.

It has also been contended that before the advent of the Aadhaar Act, no individual has been enrolled under compulsion, and since all enrolments were voluntary, they cannot be considered to be in breach of Article 21 or any other fundamental right. It is further submitted that non-adjudication of the issue of whether collection of identity information violates the right to privacy, does not prevent the Parliament from enacting a validating clause. Reliance has also been placed on **State of Karnataka** v **State of Tamil Nadu**[544] to submit that Section 59 creates a deemed fiction as a result of which one has to imagine that all actions taken under the notifications were taken under the Act.

300 Section 7 provides that the Central Government or the State Governments may require proof of an Aadhaar number as a necessary condition for availing a subsidy, benefit or service for which the expenditure is incurred from the Consolidated Fund of India. Section 3 provides that the Aadhaar number shall consist of demographic and biometric information of an

[541] (1963) 2 SCR 747
[542] (1969) 1 SCC 248
[543] (1972) 2 SCC 239
[544] (2017) 3 SCC 362

individual. “Biometric information”, under Section 2(g), means a photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by regulations. Section 4(3) provides that an Aadhaar number may be used as a proof of identity “for any purpose”. Section 57 authorizes a body corporate or person to use the Aadhaar number for establishing the identity of an individual “for any purpose”. The proviso to Section 57 provides that the use of an Aadhaar number under the Section shall be subject to the procedure and obligations under Section 8 and Chapter VI of the Act. Section 8 sets out the procedure for authentication. It states that for authentication, a requesting entity shall obtain the consent of an individual before collecting identity information and shall ensure that the identity information is only used for submission to the Central Identities Data Repository for authentication. It does not envisage collection of identity information for any other purpose. Chapter VI of the Act, which deals with protection of information, provides for security and confidentiality of identity information collected under the Act, imposes restrictions on sharing that information and classifies biometrics as sensitive personal information.

301 The scheme of the Aadhaar Act creates a system of identification through authentication of biometric information and authorises the Central and State governments to assign the task of collecting individual biometric information for the purpose of generation of Aadhaar numbers to private entities. The Act authorises the use of Aadhaar numbers by the Central

government, state governments and the private entities for establishing the identity of a resident for any purpose. The Act also contains certain safeguards regarding storage and use of biometric information. The actions taken before the enactment of the Aadhaar Act have to be tested upon the touchstone of the legal framework provided under the Act.

302 Section 59 is a validating provision. It seeks to validate all the actions of the Central Government prior to the Aadhaar Act, which were done under the notifications of 28 January 2009 and 12 September 2015. Section 59 does not validate actions of the state governments or of private entities. Acts undertaken by the State governments and by private entities are not saved by Section 59.

303 The Planning Commission's notification dated 28 January 2009 created UIDAI, while giving it the responsibility of laying down a plan and policies to implement a unique identity (UID) scheme. UIDAI was only authorized to own and operate the UID database, with a further responsibility for the updation and maintenance of the database on an ongoing basis. Significantly, the 2009 notification did not contain any reference to the use of biometrics for the purpose of the generation of Aadhaar numbers. The notification gave no authority to collect biometrics. Biometrics, finger prints or iris scans were not within its purview. There was no mention of the safeguards and measures relating to the persons or entities who would collect biometric data, how the

data would be collected and how it would be used. The website of the Press Information Bureau of the Government of India states that, by the time Aadhaar Act was notified by the Central government, UIDAI had generated about 100 crore Aadhaar numbers.[545] The collection of biometrics from individuals prior to the enactment of the Aadhaar Act does not fall within the scope of the 2009 notification. Having failed to specify finger prints and iris scans in the notification, the validating provision does not extend to the collection of biometric data before the Act. The 2009 notification did not provide authority to any government department or to any entity to collect biometrics. Since the collection of biometrics was not authorised by the 2009 notification, Section 59 of the Aadhaar Act does not validate these actions.

304 The collection of the biometrics of individuals impacts their privacy and dignity. Informed consent is crucial to the validity of a state mandated measure to collect biometric data. Encroachment on a fundamental right requires the enacting of a valid law by the legislature.[546] The law will be valid only if it meets the requirements of permissible restrictions relating to each of the fundamental rights on which there is an encroachment. Privacy animates Part III of the Constitution.[547] The invasion of any right flowing from privacy places a heavy onus upon the State to justify its actions. Nine judges of this

[545]Press Information Bureau, UIDAI generates a billion (100 crore) Aadhaars A Historic Moment for India, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=138555

[546]A Constitution Bench of this Court in State of Madhya Pradesh v. Thakur Bharat Singh (AIR 1967 SC 1170) held: "All executive action which operates to the prejudice of any person must have the authority of law to support it… Every Act done by the Government or by its officers must, if it is to operate to the prejudice of any person, be supported by some legislative authority."

[547]Puttaswamy, at para 272

Court in **Puttaswamy** categorically held that there must be a valid law in existence to encroach upon the right to privacy. An executive notification does not satisfy the requirement of a valid law contemplated in **Puttaswamy.** A valid law, in this case, would mean a law enacted by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right to privacy cannot be sustained by an executive notification.

There is also no merit in the submission of the Respondents that prior to the enactment of the Aadhaar Act, no individual has been enrolled under compulsion, and since all enrolments were voluntary, these cannot be considered to be in breach of Article 21 or any other fundamental right. The format of the first two enrolment forms used by UIDAI, under which around 90 crore enrolments were done, had no mention of informed consent or the use of biometrics. Hence, this submission is rejected.

Apart from the existence of a valid law which authorises an invasion of privacy, **Puttaswamy** requires that the law must have adequate safeguards for the collection and storage of personal data. Data protection, which is intrinsic to privacy, seeks to protect the autonomy of the individual. The judgment noted the centrality of consent in a data protection regime. The Aadhaar Act provides certain safeguards in Section 3(2) and Section 8(3) for the purposes of ensuring informed consent, and in terms of Section 29 read with Chapter VII in the form of penalties. The safeguards provided under the

Act were not in existence before the enactment of the Act. The collection of biometrics after the 2009 notification and prior to the Aadhaar Act suffers from the absence of adequate safeguards. While a legislature has the power to legislate retrospectively, it cannot retrospectively create a deeming fiction about the existence of safeguards in the past to justify an encroachment on a fundamental right. At the time when the enrolments took place prior to the enactment of the Aadhaar Act in September 2016, there was an absence of adequate safeguards. Section 59 cannot by a deeming fiction, as it were, extend the safeguards provided under the Act to the enrolments done earlier. This will be impermissible simply because the informed consent of those individuals, whose Aadhaar numbers were generated in that period cannot be retrospectively legislated by an assumption of law. Moreover, it is a principle of criminal law that it cannot be applied retrospectively to acts which were not offences at the time when they took place. Article 20(1) of the Constitution provides that “No person shall be convicted of any offence except for violation of the law in force at the time of the commission of the act charged as an offence”. The application of the criminal provisions of the Act, provided under Chapter VII of the Act which deals with “Offences and Penalties”, cannot be extended to the period prior to the enactment of the Aadhaar Act.

305 The Respondents submit that the collection of biometrics prior to the Aadhaar Act was adequately safeguarded by the provisions of the Information

Technology Act 2000; specifically those provisions, which were inserted or amended by the Information Technology (Amendment) Act, 2008.

Section 43A of the Act provides for compensation for failure to protect data:

> "Where a body corporate, possessing, dealing or handling any **sensitive personal data** or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.
>
> Explanation: For the purposes of this section,-
>
> (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
>
> (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.
>
> (iii) **"sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."**
> (Emphasis supplied)

306 Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 made by the Central government under Section 43A, defines "sensitive personal data or information":

> "Sensitive personal data or information of a person means such personal information which consists of information relating to;—
> (i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."

Section 66C provides a punishment for identity theft:

"**66C. Punishment for identity theft.-**
Whoever, fraudulently[548] or dishonestly[549] make use of the electronic signature, password or any other **unique identification feature** of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh." (Emphasis supplied)

Section 66E provides for punishment for the violation of the privacy of an individual:

"Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both."

The explanation to the Section provides that "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons.

[548]Section 25, Indian Penal Code states: ""Fraudulently".—A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise"
[549]Section 24, Indian Penal Code states: ""Dishonestly"- Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly"

"Capture", with respect to an image, has been defined to mean videotaping, photographing, filming or recording by any means. "Private area" means the "naked or undergarment clad genitals, pubic area, buttocks or female breast." "Publishes" has been defined as reproduction in the printed or electronic form and making it available for public.

Section 72A provides for punishment for disclosure of information in breach of a lawful contract:

> "Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material **to any other person** shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both." (Emphasis supplied)

Section 43A applies only to bodies corporate and has no application to government or to its departments. Explanation (i) defines body corporate to mean any company and to include a firm, sole proprietorship or other association of individuals engaged in professional or commercial activities. Personal information leaked or lost by government agencies will not be covered under Section 43A. The scope of Section 66E is limited. It only deals with the privacy of the "private area" of any person. It does not deal with informational privacy. The scope of Section 72A is also limited. It only penalises acts of disclosing personal information about a person obtained

while providing services under a lawful contract. Section 66C deals with identity theft and punishes the dishonest or fraudulent use of the unique identification feature of a person. The Information Technology Act also does not penalise unauthorised access to the Central Identities Data Repository. Many of the safeguards which were introduced by the Aadhaar Act were not comprehended in the provisions of the Information Technology Act. Indeed, it was the absence of those safeguards in the Information Technology Act which required their introduction in the Aadhaar Act. Hence, the Attorney General is not correct in submitting that India operated under a regime of comprehensive safeguards governing biometric data during the period when the Aadhaar project was governed by an executive notification, in the absence of a legislative framework. The absence of a legislative framework rendered the collection of biometric data vulnerable to serious violations of privacy. There are two distinct facets here. First, the absence of a legislative framework for the Aadhaar project between 2009 and 2016 left the biometric data of millions of Indian citizens bereft of the kind of protection which a law, as envisaged in **Puttaswamy**, must provide to comprehensively protect and enforce the right to privacy. Second, the notification of 2009 does not authorise the collection of biometric data. Consequently, the validation of actions taken under the 2009 notification by Section 59 does not save the collection of biometric data prior to the enforcement of the Act. Privacy is of paramount importance. No invasion of privacy can be allowed without proper, adequate and stringent

safeguards providing not only penalties for misuse or loss of one's personal information, but also for protection of that person.

307 The Respondents have relied upon several judgments where this Court has upheld validating statutes, which, they contend, are similar to Section 59. The first decision which needs to be discussed is the judgment of the Constitution Bench in **West Ramnad,** which dealt with a validating statute of the Madras Legislature. Act 43 of 1949 of the Madras Legislature which sought to acquire electricity undertakings in the state was struck down for want of legislative competence. In the meantime, the Constitution came into force, and under the Seventh Schedule, the State acquired legislative competence. A fresh law was enacted in 1954. Section 24 sought to validate actions done and taken under the 1949 Act. Section 24 provided thus:

> "Orders made, decisions or directions given, notifications issued, proceedings taken and acts or things done, in relation to any undertaking taken over, **if they would have been validly made, given, issued, taken or done, had the Madras Electricity Supply Undertakings (Acquisition) Act 1949 (Madras Act 43 of 1949), and the rules made thereunder been in force on the date on which the said orders**, decisions or directions, notifications, proceeding, acts or things were made, given, issued, taken or done are **hereby declared to have been validly made, given, issued, taken or done, as the case may be, except to the extent to which the said orders, decisions, directions, notifications, proceedings, acts or things are repugnant to the provisions of this Act.**" (Emphasis supplied)

Section 24 was held to be a provision, which saved and validated actions validly taken under the provisions of the earlier Act, which was invalid from the

inception. Justice Gajendragadkar, speaking for the Court, interpreted Section 24 thus:

> "12. The first part of the section deals, inter alia, with **notifications which have been validly issued under the relevant provisions of the earlier Act** and it means that if the earlier Act had been valid at the relevant time, it ought to appear that the notifications in question could have been and had in fact been made properly under the said Act. **In other words, before any notification can claim the benefit of Section 24, it must be shown that it was issued properly under the relevant provisions of the earlier Act, assuming that the said provisions were themselves valid and in force at that time.** The second part of the section provides that the notifications covered by the first part are declared by this Act to have been validly issued; the expression "hereby declared" clearly means "declared by this Act" and that shows that the notifications covered by the first part would be treated as issued under the relevant provisions of the Act and would be treated as validly issued under the said provisions. The third part of the section provides that the statutory declaration about the validity of the issue of the notification would be subject to this exception that the said notification should not be inconsistent with or repugnant to the provisions of the Act. **In other words, the effect of this section is that if a notification had been issued properly under the provisions of the earlier Act and its validity could not have been impeached if the said provisions were themselves valid, it would be deemed to have been validly issued under the provisions of the Act, provided, of course, it is not inconsistent with the other provisions of the Act.** The section is not very happily worded, but on its fair and reasonable construction, there can be no doubt about its meaning or effect." (Emphasis supplied)

308 The second decision is a four judge Bench judgment in **Chetty**, which dealt with the competence of a legislature to remedy a discriminatory procedure retrospectively. There were two Acts in Mysore for acquisition of private land for public purposes – the Mysore Land Acquisition Act, 1894 and the City of Bangalore Improvement Act, 1945. The respondent challenged a notification which was issued under the 1894 Act for the acquisition of his land

in Bangalore, on the ground that recourse to the provisions of the Land Acquisition Act was discriminatory because in other cases the provisions of the Improvement Act were applied. The High Court accepted the contention, against which there was an appeal to this Court. During the pendency of the appeal, the Bangalore Acquisition of Lands (Validation) Act, 1962 was passed. The 1962 Act contained two provisions. Section 2 provided:

> "2. *Validation of certain acquisition of lands and proceedings and orders connected therewith.-*
>
> (1) Notwithstanding anything contained in the City of Bangalore Improvement Act, 1945 (Mysore Act 5 of 1945), or in any other law, or in any judgment, decree or order of any court:
>
> (a) every acquisition of land for the purpose of improvement, expansion or development of the City of Bangalore or any area to which the City of Bangalore Improvement Act, 1945, extends, **made by the State Government acting or purporting to act under the Mysore Land Acquisition Act, 1894 (Mysore Act 7 of 1894)**, at any time before the commencement of this Act, and every proceeding held, notification issued and order made in connection with the acquisition of land for the said purpose **shall be deemed for all purposes to have been validly made, held to issue, as the case may be, and any acquisition proceeding commenced under the Mysore Land Acquisition Act, 1894**, for the said purpose before the commencement of this Act but not concluded before such commencement, may be continued under the Land Acquisition Act, 1894 (Central Act 1 of 1894), as extended to the State of Mysore by the Land Acquisition (Mysore Extension and Amendment) Act, 1961, and accordingly no acquisition so made, no proceeding held, no notification issued and no order made by the State Government or by any authority under the Mysore Land Acquisition Act, 1894, or the Land Acquisition Act, 1894, in connection with any such acquisition shall be called in question on the ground that the State Government was not competent to make acquisition of land for the said purpose under the said Act or on any other ground whatsoever;
>
> (b) any land to the acquisition of which the provisions of clause (a) are applicable shall, after it has vested in the State Government, be deemed to have been

> transferred, or stand transferred, as the case may be, to the Board of Trustees for the improvement of the City of Bangalore." (Emphasis supplied)

The Act of 1962 validated all acquisitions made, proceedings held, notifications issued or orders made under the Mysore Land Acquisition Act before the validating law came into force. The Validation Act was challenged on the ground that it was discriminatory to provide two Acts which prescribed two different procedures under the acquisition laws in the same field. This Court found that the legislature retrospectively made a single law for the acquisition of properties and upheld the validating Act. It was held:

> "15. If two procedures exist and one is followed and the other discarded, there may in a given case be found discrimination. But the Legislature has still the competence to put out of action retrospectively one of the procedures leaving one procedure only available, namely, the one followed and thus to make disappear the discrimination. In this way a Validating Act can get over discrimination. Where, however, the legislative competence is not available, the discrimination must remain for ever, since that discrimination can only be removed by a legislature having power to create a single procedure out of two and not by a legislature which has not that power."

309 In **West Ramnad**, the validation depended upon the condition that a notification or act ought to have been validly issued or done under the earlier statute, presuming that the earlier Act was itself valid at that time. In the present case, there was no earlier law governing the actions of the government for the collection of biometric data. The Aadhaar Act was notified in 2016. The Planning Commission's notification of 2009 and the Ministry of Information and Technology's notification of 2015 were not issued under any

statute. Therefore, the validating law in **West Ramnad** was clearly of a distinct genre. **West Ramnad** will be of no assistance to the Union of India.

310 The decision in **Chetty** in fact brings out the essential attributes of a validating law. The existence of two legislations governing the field of land acquisition had been found to be discriminatory and hence violative of Article 14 by the High Court (on the basis of the position in law as it then stood). During the pendency of the appeal before this Court, the legislature enacted a validating law which removed the cause for invalidity. The reason the state law had been invalidated by the High Court was the existence of two laws governing the same field. This defect was removed. To use the words of this Court, the legislature "put out of action retrospectively one of the procedures" as a result of which only one procedure was left in the field. The decision in **Chetty** thus brings out the true nature of a validating law. A validating law essentially removes the deficiency which is found to exist in the earlier enactment. By curing the defect, it validates actions taken under a previous enactment.

311 The third judgment of seven judges is in **Hari Singh**. The constitutionality of the Public Premises (Eviction of Unauthorised Occupants) Act, 1958 was challenged on the ground that Section 5(1) contravened Article 14. Section 5(1) conferred power on the Estate Officer to make an order of eviction against persons who were in unauthorised occupation of public

premises. During the pendency of the appeal before this Court, the Public Premises (Eviction of Unauthorised Occupants) Act, 1971 was enacted, which validated all actions taken under the Act of 1958. The constitutional validity of the 1971 Act was also challenged. Section 20 of the later Act provided:

> "Notwithstanding any judgment, decree or order of any court, **anything done or any action taken** (including rules or orders made, notices issued, evictions ordered or effected, damages assessed, rents or damages or costs recovered and proceedings initiated) **or purported to have been done or taken under the Public Premises (Eviction of Unauthorised Occupants) Act, 1958 shall be deemed to be as valid and effective as if such thing or action was done or taken under the corresponding provisions of this Act** which, under Sub-section (3) of Section 1 **shall be deemed to have come into force on the 16th day of September, 1958** ..." (Emphasis supplied)

The Court held that the legislature has the power to validate actions under an earlier law by removing its infirmities. In that case, validation was achieved by enacting the 1971 Act with retrospective effect from 1958 and legislating that actions taken under the earlier law will be deemed to be as valid and effective as if they were taken under the 1971 Act. The Court held:

> "24. The 1958 Act has not been declared by this Court to be unconstitutional… The arguments on behalf of the appellants therefore proceeded on the footing that the 1958 Act will be presumed to be unconstitutional. It was therefore said that the 1971 Act could not validate actions done under the 1958 Act. The answer is for the reasons indicated above that the Legislature was competent to enact this legislation in 1958 and the Legislature by the 1971 Act has given the legislation full retrospective operation. The Legislature has power to validate actions under an earlier Act by removing the infirmities of the earlier Act. The 1971 Act has achieved that object of validation."

The Court approved the Constitution Bench decision in **West Ramnad**:

> "16. The ruling of this Court in West Ramnad Electric Distribution Co. Ltd. case establishes competence of the legislature to make laws retrospective in operation for the purpose of validation of action done under an earlier Act which has been declared by a decision of the court to be invalid. It is to be appreciated that the validation is by virtue of the provisions of the subsequent piece of legislation."

In **Hari Singh**, the validating Act retrospectively authorised the actions undertaken under the previous Act, which had been invalidated by a court decision. The validating law of 1971 was enacted with retrospective effect from 1958.

312 Reliance was placed by the Respondents on the judgments of this Court in **Jaora Sugar Mills (P) Ltd.** v **State of Madhya Pradesh**[550] **(Jaora Sugar Mills)**, **SKG Sugar Ltd.** v **State of Bihar**[551] **("SKG Sugar")** and **Krishna Chandra Gangopadhyaya** v **Union of India**[552] **("Krishna Chandra")**, to contend that in the case of fiscal legislation, where an enactment was struck down for violating Article 265 or the fundamental rights, of a citizen, validating Acts were enacted after removing the flaw and that in cases where the state Legislature was held to be incompetent to enact a taxing measure, a validating law was enacted by Parliament by making a substantive provision.

[550] (1966) 1 SCR 523
[551] (1974) 4 SCC 827
[552] (1975) 2 SCC 302

313 In **Jaora Sugar Mills**, a state law imposing cess was struck down for want of legislative competence. Parliament enacted the Sugarcane Cess (Validation) Act, 1961 to validate the imposition of cess under the invalidated state law. Section 3(1) of the 1961 Act provided:

> "12…Notwithstanding any judgment, decree or order of any Court, all cesses imposed, assessed or collected or purporting to have been imposed, assessed or collected **under any State Act** before the commencement of this act **shall be deemed to have been validly imposed,** assessed or collected in accordance with law, **as if the provisions of the State Acts** and of all notifications, orders and rules issued or made thereunder, in so far as such provisions relate to the imposition, assessment and collection of such cess had been included in and **formed part of this section and this section had been in force at all material times when such cess was imposed, assessed or collected**; …." (Emphasis supplied)

The Section was upheld. Speaking for the Constitution Bench, Chief Justice Gajendragadkar held:

> "14... What Parliament has done by enacting the said section is not to validate the invalid State Statutes, but **to make a law concerning the cess covered by the said Statutes and to provide that the said law shall come into operation retrospectively.** There is a radical difference between the two positions. Where the legislature wants to validate an earlier Act which has been declared to be invalid for one reason or another, it proceeds to remove the infirmity from the said Act and validates its provisions which are free from any infirmity." (Emphasis supplied)

The state law was held to be invalid for want of legislative competence. Parliament, which was competent to enact a law on the subject, did so with retrospective effect and validated actions which were taken under the invalid state law.

314 In **SKG Sugar,** a state law - Bihar Sugar Factories Control Act, 1937 - was declared unconstitutional. In 1969, during President's Rule in Bihar, Parliament enacted the Bihar Sugarcane (Regulation of Supply and Purchase) Act, 1969. Section 66(1) of the Act provided:

> "12…Notwithstanding any judgment, decree or order of any court, **all cesses and taxes imposed**, assessed or collected or purporting to have been imposed, assessed or collected **under any State law**, before the commencement of this Act, **shall be deemed to have been validly imposed**, assessed or collected in accordance with law **as if this Act had been in force at all material times** when such cess or tax was imposed, assessed or collected and accordingly...."[553] (Emphasis supplied)

The Constitution Bench held:

> "32… By virtue of the legal fiction introduced by the validating provision in Section 66(1), the impugned notification will be deemed to have been issued not necessarily under the Ordinance No. 3 of 1968 but under the President's Act, itself, deriving its legal force and validity directly from the latter."[554]

315 In **Krishna Chandra**, provisions of the Bihar Land Reforms Act, 1950 were struck down for want of legislative competence. Parliament enacted the Mines and Minerals (Regulation and Development) Act, 1957 to validate those provisions with retrospective effect. Section 2 provided that:

> "1…(2). **Validation of certain Bihar State laws and action taken and things done connected therewith.-**
> (1) **The laws specified in the schedule shall be and shall be deemed always to have been, as valid as if the provisions contained therein had been enacted by Parliament.**
> (2) Notwithstanding any judgment, decree or order of any court, **all actions taken**, things done, rules made, notifications issued or purported to have been taken, done,

[553] Ibid, at page 831
[554] Ibid, at page 835

> made or issued and rents or royalties realised **under any such laws shall be deemed to have been validly taken, done**, made, issued or realised, as the case may be, as if this **section had been in force at all material times when such action was taken,** things were done, rules were, made, notifications were issued, or rents or royalties were realised, and no suit or other proceedings shall be maintained or continued in any court for the refund of rents or royalties realised under any such laws.
> (3) For the removal of doubts, it is hereby declared that nothing in Sub-section (2) shall be construed as preventing any person from claiming refund of any rents or royalties paid by him in excess of the amount due from him under any such laws."[555] (Emphasis supplied)

The central issue in the case was whether a statute and a rule earlier declared to be unconstitutional or invalid, can be retroactively enacted through fresh validating legislation by the competent Legislature. The Court held that it could be.

316 Section 59 of the Aadhaar Act is different from the validating provisions in **Jaora Sugar Mills**, **SKG Sugar** and **Krishna Chandra.** In those cases, state laws were invalid for want of legislative competence. Parliament, which undoubtedly possessed legislative competence, could enact a fresh law with retrospective effect and protect actions taken under the state law. The infirmity being that the earlier laws were void for absence of competence in the legislature, the fresh laws cured the defect of the absence of legislative competence.

[555] Ibid, at page 306

317 Parliament and the State Legislatures have plenary power to legislate on subjects which fall within their legislative competence. The power is plenary because the legislature can legislate with prospective as well as with retrospective effect. Where a law suffers from a defect or has been invalidated, it is open to the legislature to remove the defect. While doing that, the legislature can validate administrative acts or decisions made under the invalid law in the past. The true test of a validation is that it must remove the defects in the earlier law. It is not enough for the validating law to state that the grounds of invalidity of the earlier law are deemed to have been removed. The validating law must remove the deficiencies. There were several deficiencies in the collection of biometric data during the period between 2009 and 2016, before the Aadhaar Act came into force. The first was the absence of enabling legislation. As a result, the collection of sensitive personal information took place without the authority of law. Second, the notification of 2009 did not authorize the collection of biometric data. Third, the collection of biometric data was without an enabling framework of the nature which the Aadhaar Act put into place with effect from 2016. The Aadhaar Act introduced a regime for obtaining informed consent, securing the confidentiality of information collected from citizens, penalties and offences for breach and regulated the uses to which the data which was collected could be put. In the absence of safeguards, the collection of biometric data prior of the enactment of Aadhaar Act 2016 is *ultra vires*.

318 Section 59 does not remove the cause for invalidity. First, Section 59 protects actions taken under the notification of 2009. The notification does not authorize the collection of biometric data. Hence, Section 59 would not provide legal authority for the collection of biometrics between 2009 and 2016. Second, it was through the Aadhaar Act, that safeguards were sought to be introduced for ensuring informed consent, confidentiality of information collected, restrictions on the use of the data and through a regime of penalties and offences for violation. Section 59 does not cure the absence of these safeguards between 2009 and 2016. Section 59 fails to meet the test of a validating law for the simple reason that the absence of safeguards and of a regulatory framework is not cured merely by validating what was done under the notifications of 2009 and 2016. There can be no dispute about the principle that the legislature is entitled to cure the violation of a fundamental right. But in order to do so, it is necessary to cure the basis or the foundation on which there was a violation of the fundamental right. The deficiency must be demonstrated to be cured by the validating law. Section 59 evidently fails to do so. It fails to remedy the deficiencies in regard to the conditions under which the collection of biometric data took place before the enforcement of the Aadhaar Act in 2016.

The Respondents submitted that Section 59 creates a deemed fiction and cited a few judgments in support of this contention. In **Bishambhar Nath**

Kohli v **State of Uttar Pradesh**[556], an Ordinance repealed another Ordinance. Section 58(3) of the repealing Ordinance stated:

> "6…The repeal by this Act of the Administration of Evacuee Property Ordinance, 1949 or the Hyderabad Administration of Evacuee Property Regulation or of any corresponding law shall not affect the previous operation of that Ordinance, Regulation or corresponding law, and subject thereto, anything done or **any action taken in the exercise of any power conferred by or under that Ordinance, Regulation or corresponding law, shall be deemed to have been done or taken in the exercise of the powers conferred by or under this Act as if this Act were in force on the day on which such thing was done or action was taken.**" (Emphasis supplied)

319 A Constitution Bench of this Court held that by virtue of Section 58, all things done and actions taken under the repealed ordinance are deemed to be done or taken in exercise of the powers conferred by the repealing Act, as if that Act were in force on the day on which that thing was done or action was taken. The things done or actions taken under the repealed ordinance are to be deemed by fiction to have been done or taken under the repealing Act. The actions were validated because the Act, in this case, was deemed to be "in force on the day on which such thing was done or action was taken". Section 59 of the Aadhaar Act does not create this fiction. The Aadhaar Act does not come in force on the date on which the actions, which this Section seeks to validate, were taken.

320 A three judge Bench headed by one of us, Hon'ble Mr Justice Dipak Misra (as the learned Chief Justice then was) in **State of Karnataka** v **State**

[556] (1966) 2 SCR 158

of Tamil Nadu[557], was dealing with a batch of civil appeals filed against a final order of the Cauvery Water Disputes Tribunal constituted under the Inter-State River Water Disputes Act, 1956. Section 6(2) of the 1956 Act provides:

> "72…6(2).The decision of the Tribunal, after its publication in the Official Gazette by the Central Government under Sub-section (1), shall have the same force as an order or decree of the Supreme Court."[558]

Relying on Section 6(2), it was contended that the jurisdiction of this Court is ousted as it cannot sit in appeal on its own decree. The Court did not accept the submission and held:

> "74. The language employed in Section 6(2) suggests that the decision of the tribunal shall have the same force as the order or decree of this Court. There is a distinction between having the same force as an order or decree of this Court and passing of a decree by this Court after due adjudication. The Parliament has intentionally used the words from which it can be construed that a legal fiction is meant to serve the purpose for which the fiction has been created and **not intended to travel beyond it.** The purpose is to have the binding effect of the tribunal's award and the effectiveness of enforceability. Thus, it has to be narrowly construed regard being had to the purpose it is meant to serve…[559]
>
> 81…it is clear as crystal that the Parliament did not intend to create any kind of embargo on the jurisdiction of this Court. The said provision was inserted to give the binding effect to the award passed by the tribunal. **The fiction has been created for that limited purpose.**"[560] (Emphasis supplied)

The judgment makes it clear that a deeming fiction cannot travel beyond what was originally intended. As stated earlier, the action of collecting and authentication of biometrics or the requirement of informed consent finds no

[557] (2017) 3 SCC 362
[558] Ibid, at page 405
[559] Ibid, at page 406
[560] Ibid, at page 408

mention in the 2009 notification. Therefore, Section 59 cannot be held to create a deeming fiction that all the actions taken under the notifications issued were done under the Act and not under the aforesaid notifications.

321 This Court must also deal with the Respondents' submission that Parliament is not debarred from enacting a validation law even though the Court did not have the opportunity to rule on the validity of the notifications which are purported by Section 59 to have been validated. The Respondents have placed reliance on a two judge Bench decision in **Amarendra Kumar Mohapatra** v **State of Orissa**.[561] This case involved a challenge to the constitutional validity of the Orissa Service of Engineers (Validation of Appointment) Act, 2002 enacted to regularise *ad hoc* appointments of employees. The issue before the Court was whether the Orissa Act was in effect a validation statute to validate any illegality or defect in a pre-existing Act or rule in existence. The Court held that since the Orissa Act merely regularised the appointment of graduate Stipendiary Engineers working as *ad hoc* Assistant Engineers as Assistant Engineers, it could not be described as a validating law. It was held the legislation did not validate any such non-existent act, but simply appointed the ad hoc Assistant Engineers as substantive employees of the State by resort to a fiction. This Court held:

> "31…a prior judicial pronouncement declaring an act, proceedings or rule to be invalid is not a condition precedent for the enactment of a Validation Act. Such a piece of legislation may be enacted to remove even a perceived invalidity, which the Court has had no opportunity to adjudge.

[561] (2014) 4 SCC 583

> Absence of a judicial pronouncement is not, therefore, of much significance for determining whether or not the legislation is a validating law."[562]

The Court further held that:

> "25. … when the validity of any such Validation Act is called in question, **the Court would have to carefully examine the law and determine whether (i) the vice of invalidity that rendered the act, rule, proceedings or action invalid has been cured by the validating legislation (ii) whether the legislature was competent to validate the act, action, proceedings or rule declared invalid in the previous judgments and (iii) whether such validation is consistent with the rights guaranteed by Part III of the Constitution.** It is only when the answer to all these three questions is in the affirmative that the Validation Act can be held to be effective and the consequences flowing from the adverse pronouncement of the Court held to have been neutralised." (Emphasis supplied)

322 The two judge Bench relied upon the Constitution Bench decision of this Court in **Shri Prithvi Cotton Mills Ltd** v **Broach Borough Municipality**[563] to formulate the following pre-requisites of a piece of legislation that purports to validate any act, rule, action or proceedings:

> "(a) The legislature enacting the Validation Act should be competent to enact the law and;
> (b) the cause for ineffectiveness or invalidity of the Act or the proceedings needs to be removed."

These judgments suggest that while there can be no disagreement with the proposition that a legislature has the power, within its competence, to make a law to validate a defective law, the validity of such a law would depend upon whether it removes the cause of ineffectiveness or invalidity of the previous

[562] Ibid, at page 604
[563] (1969) 2 SCC 283

Act or proceedings. Parliament has the power to enact a law of validation to cure an illegality or defect in the pre-existing law, with or without a judicial determination. But that law should cure the cause of infirmity or invalidity. Section 59 fails to cure the cause of invalidity prior to the enactment of the Aadhaar Act.

K Rule of law and violation of interim orders

323 The rule of law is the cornerstone of modern democratic societies and protects the foundational values of a democracy. When the rule of law is interpreted as a principle of constitutionalism, it assumes a division of governmental powers or functions that inhibits the exercise of arbitrary State power. It also assumes the generality of law: the individual's protection from arbitrary power consists in the fact that her personal dealings with the State are regulated by general rules, binding on private citizens and public officials alike.[564]

It envisages a fundamental separation of powers among different organs of the State. Separation of power supports the accountability aspect of the rule of law. Separation of the judicial and executive powers is an essential feature of the rule of law. By entrusting the power of judicial review to courts, the doctrine prevents government officials from having the last word on whether

[564]T. R. S. Allan, Constitutional Justice: A Liberal Theory of the Rule of Law (2001), available at http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199267880.001.0001/acprof-9780199267880-chapter-2

they have acted illegally. The separation of judicial power provides an effective check on the executive branch.[565]

324 The concepts of the rule of law and separation of powers have been integral to Indian constitutional discourse. While both these concepts have not been specified in as many words in the Constitution, they have received immense attention from this Court in its judgments. Though the Indian Constitution does not follow the doctrine of separation of powers in a rigid sense, the following statement of the law by Chief Justice Mukherjea in **Ram Sahib Ram Jawaya Kapur** v **State of Punjab**[566] is widely regarded as defining the core of its content:

> "12…The Indian Constitution has not indeed recognised the doctrine of separation of powers in its absolute rigidity but the functions of the different parts or branches of the Government have been sufficiently differentiated and consequently it can very well be said that our Constitution does not contemplate assumption, by one organ or part of the State, of functions that essentially belong to another..."

Separation of powers envisages a system of checks and balances, which ensures governance by law and not by the caprice of those to whom governance is entrusted for the time being. By curbing excesses of power, it has a direct link with the preservation of institutional rectitude and individual liberty. In **S G Jaisinghani** v **Union of India**[567], this Court held that:

> "14. In this context it is important to emphasize that the absence of arbitrary power is the first essential of the rule of

[565]Denise Meyerson, The Rule of Law and the Separation of Powers (2004), available at http://www5.austlii.edu.au/au/journals/MqLJ/2004/1.html
[566] (1955) 2 SCR 225
[567] (1967) 2 SCR 703

> law upon which our whole constitutional system is based. In a system governed by rule of law, discretion, when conferred upon executive authorities, must be confined within clearly defined limits. The rule of law from this point of view means that decisions should be made by the application of known principles and rules and, in general, such decisions should be predictable and the citizen should know where he is. If a decision is taken without any principle or without any rule it is unpredictable and such a decision is the antithesis of a decision taken in accordance with the Rule of law…"

The separation of powers between the legislature, the executive and the judiciary has been declared to be part of the basic structure of the Constitution. In **Kesavananda Bharati** v **State of Kerala**[568], Chief Justice Sikri held that:

> "292…The basic structure may be said to consist of the following features:
> **(1) Supremacy of the Constitution;**
> (2) Republican and Democratic form of Government;
> (3) Secular character of the Constitution;
> **(4) Separation of powers between the legislature, the executive and the judiciary;**
> (5) Federal character of the Constitution."[569]
> (Emphasis supplied)

Justice HR Khanna held that the rule of law meant "supremacy of the Constitution and the laws as opposed to arbitrariness"[570]. The same view is expressed in subsequent decisions of this Court.[571] In **Smt Indira Nehru Gandhi** v **Shri Raj Narain**[572], Chief Justice AN Ray held the rule of law to be the basis of democracy.

---

[568] (1973) 4 SCC 225
[569] Ibid, at page 366
[570] Ibid, at para 1529
[571] Smt. Indira Nehru Gandhi v. Shri Raj Narain, 1975 (Supp.) SCC 1; State of Bihar v. Bal Mukund Sah, (2000) 4 SCC 640]; I .R. Coelho (Dead) by L.Rs. v. State of Tamil Nadu, (2007) 2 SCC 1.
[572] 1975 Supp SCC 1

The functional relationship between separation of powers and the rule of law was discussed by a Constitution Bench of this Court in **State of Tamil Nadu** v **State of Kerala**[573], as follows:

> "98. Indian Constitution, unlike the Constitution of United States of America and Australia, does not have express provision of separation of powers. However, the structure provided in our Constitution leaves no manner of doubt that the doctrine of separation of powers runs through the Indian Constitution. It is for this reason that this Court has recognized separation of power as a basic feature of the Constitution and an essential constituent of the rule of law. The doctrine of separation of powers is, though, not expressly engrafted in the Constitution, its sweep, operation and visibility are apparent from the Constitution. Indian Constitution has made demarcation without drawing formal lines between the three organs--legislature, executive and judiciary."

This Court has consistently held judicial review to be an essential component of the separation of powers as well as of the rule of law. Judicial review involves determination not only of the constitutionality of law but also of the validity of administrative action. It protects the essence of the rule of law by ensuring that every discretionary power vested in the executive is exercised in a just, reasonable and fair manner.

325 In a **reference**[574] under Article 143 of the Constitution, a seven judge Bench held that irrespective of "whether or not there is distinct and rigid separation of powers under the Indian Constitution", the judicature has been entrusted the task of construing the provisions of the Constitution and of safeguarding the fundamental rights of citizens. It was held:

[573] (2014)12 SCC 696
[574] (1965) 1 SCR 413

> "41…When a statute is challenged on the ground that it has been passed by Legislature without authority, or has otherwise unconstitutionally trespassed on fundamental rights, it is for the courts to determine the dispute and decide whether the law passed by the legislature is valid or not… If the validity of any law is challenged before the courts, it is never suggested that the material question as to whether legislative authority has been exceeded or fundamental rights have been contravened, can be decided by the legislatures themselves. Adjudication of such a dispute is entrusted solely and exclusively to the Judicature of this country…"

In his celebrated dissent in **Additional District Magistrate, Jabalpur** v **Shivakant Shukla**[575], Justice HR Khanna, while referring to the rule of law as the "antithesis of arbitrariness", held:

> "527…Rule of law is now the accepted norm of all civilised societies... [E]verywhere it is identified with the liberty of the individual. It seeks to maintain a balance between the opposing notions of individual liberty and public order. In every State the problem arises of reconciling human rights with the requirements of public interest. Such harmonising can only be attained by the existence of independent courts which can hold the balance between citizen and State and compel Governments to conform to the law."[576]

326 Judicial review has been held to be one of the basic features of the Constitution. A seven judge Bench of this Court, in **L Chandra Kumar** v **Union of India**[577], declared:

> "78… the power of judicial review over legislative action vested in the High Courts under Article 226 and in the Supreme Court under Article 32 of the Constitution is an integral and essential feature of the Constitution, constituting part of its basic structure."[578]

[575] (1976) 2 SCC 521
[576] Ibid, at page 748
[577] (1997) 3 SCC 261
[578] Ibid, at page 301

The complementary relationship between judicial review, the rule of law and the separation of powers is integral to working of the Constitution. This Court in **I R Coelho** v **State of Tamil Nadu**[579] held thus:

> "129… Equality, rule of law, judicial review and separation of powers form parts of the basic structure of the Constitution. Each of these concepts are intimately connected. There can be no rule of law, if there is no equality before the law. These would be meaningless if the violation was not subject to the judicial review. All these would be redundant if the legislative, executive and judicial powers are vested in one organ. Therefore, the duty to decide whether the limits have been transgressed has been placed on the judiciary."[580]

Judicial review, by protecting individual rights, promotes the foundational values of the Constitution and the rule of law. This Court took note of this aspect in **Puttaswamy**:

> *"*295. Above all, it must be recognized that judicial review is a powerful guarantee against legislative encroachments on life and personal liberty. To cede this right would dilute the importance of the protection granted to life and personal liberty by the Constitution. Hence, while judicial review in constitutional challenges to the validity of legislation is exercised with a conscious regard for the presumption of constitutionality and for the separation of powers between the legislative, executive and judicial institutions, the constitutional power which is vested in the Court must be retained as a vibrant means of protecting the lives and freedoms of individuals."[581]

327 Constitutional adjudication facilitates answers to the silences of the Constitution. The task of interpretation is to foster the spirit of the Constitution as much as its text. This role has exclusively been conferred on the Supreme Court and the High Courts to ensure that its values are not diminished by the

[579] (2007) 2 SCC 1
[580] Ibid, at page 58
[581] Ibid, at page 497

legislature or the executive. Our Court has been conscious of this role. In **Krishna Kumar Singh** v **State of Bihar**[582], while dealing with the question whether an ordinance (promulgated by the Governor) which has a limited life can bring about consequences for the future (in terms of the creation of rights, privileges, liabilities and obligations) which will enure beyond its life, a seven judge Bench held that:

> "91…**The silences of the Constitution must be imbued with substantive content by infusing them with a meaning which enhances the Rule of law.** To attribute to the executive as an incident of the power to frame ordinances, an unrestricted ability to create binding effects for posterity would set a dangerous precedent in a parliamentary democracy. The court's interpretation of the power to frame ordinances, which originates in the executive arm of government, cannot be oblivious to the basic notion that the primary form of law making is through the legislature..."[583] (Emphasis supplied)

The Court held that the ordinance making power must be carefully structured to ensure that it remains what the framers of our Constitution intended it to be: an exceptional power to meet a constitutional necessity.

328 In a constitutional democracy, the power of government, is defined, limited, and distributed by the fundamental norms of the Constitution. A constitutional democracy holds its political regime accountable, responsible, or answerable for its decisions and actions while in public office.[584] A

[582] (2017) 3 SCC 1
[583] Ibid, at page 76
[584] Almon Leroy Way, Jr., Constitutional Democracy & Other Political Regimes, available at http://www.proconservative.net/CUNAPolSci201PartTWOA.shtml

constitutional democracy determines the degree and manner of distribution of political authority among the major organs or parts of the government. The limits of each institution are set by the Constitution. No institution which has been created by the Constitution can have absolute power. Separation of powers, envisaged by the Constitution between different institutions acts as a check and balance among the institutions and promotes the rule of law by ensuring that no institution can act in an arbitrary manner. Judicial review as a part of the basic structure of the Indian Constitution and as an essential component of the rule of law and separation of powers, is intended to ensure that every institution acts within its limits. Judicial review promotes transparency, consistency and accountability in the administration of law, and notions of equity, justice and fairness[585]. Constitutionalism thus puts a legal limitation on the government. It envisages the existence of limited government. Discretion conferred upon an institution of governance, be it the legislature or the executive, is confined within clearly defined limits of the Constitution. Not only are the organs of the State required to operate within their defined legitimate spheres; they are bound to exercise their powers within these spheres without violating the Constitution.[586] Judicial review is a sanction and agency to enforce the limitations imposed by the Constitution upon the authority of the organs of the State.

[585]In Sheela Barse v. State of Maharashtra ((1983) 2 SCC 96), the Supreme Court insisted on fairness to women in police lock-up and also drafted a code of guidelines for the protection of prisoners in police custody, especially female prisoners. In Veena Sethi v. State of Bihar (AIR 1982 S.C. 1470), the Supreme Court extended the reach of rule of law to the poor who constitute the bulk of India by ruling that rule of law does not merely for those who have the means to fight for their rights and expanded the locus standi principle to help the poor

[586]Durga Das Basu, Limited Government and Judicial Review, LexisNexis, (2016) at pages 123-124

This formulation of the limited power of political authority has been recognized in several judgments of this Court. In **State of M P** v **Thakur Bharat Singh**[587], a Constitution Bench held:

> "5…Our federal structure is founded on certain fundamental principles: (1) **the sovereignty of the people with limited Government authority** i.e. the Government must be conducted in accordance with the will of the majority of the people. The people govern themselves through their representatives, whereas the official agencies of the executive Government possess only such powers as have been conferred upon them by the people; (2) **There is a distribution of powers between the three organs of the State — legislative, executive and judicial — each organ having some check direct or indirect on the other; and (3) the rule of law which includes judicial review of arbitrary executive action…**" (Emphasis supplied)

329 In a decision rendered by a Constitution Bench, in **S P Sampath Kumar** v **Union of India**[588], Chief Justice P.N. Bhagwati, in his concurring opinion, held:

> "3…It is a fundamental principle of our constitutional scheme that every organ of the State, every authority under the Constitution, derives its power from the Constitution and has to act within the limits of such power. It is a limited government which we have under the Constitution and both the executive and the legislature have to act within the limits of the power conferred upon them under the Constitution… **The judiciary is constituted the ultimate interpreter of the Constitution and to it is assigned the delicate task of determining what is the extent and scope of the power conferred on each branch of government, what are the limits on the exercise of such power under the Constitution and whether any action of any branch**

[587](1967) 2 SCR 454
[588] (1987) 1 SCC 124

> **transgresses such limits.** It is also a basic principle of the rule of law which permeates every provision of the Constitution and which forms its very core and essence that the exercise of power by the executive or any other authority must not only be conditioned by the Constitution but also be in accordance with law and it is the judiciary which has to ensure that the law is observed and there is compliance with the requirements of law on the part of the executive and other authorities…"[589] (Emphasis supplied)

330 In **I R Coelho** v **State of Tamil Nadu**[590], a nine judge Bench held that control over government power ensures that the foundational values of a democracy are not damaged:

> "43…The principle of constitutionalism advocates a check and balance model of the separation of powers; it requires a diffusion of powers, necessitating different independent centres of decision-making… The role of the judiciary is to protect fundamental rights. A modern democracy is based on the twin principles of majority rule and the need to protect fundamental rights. According to Lord Steyn, it is job of the judiciary to balance the principles ensuring that the Government on the basis of number does not override fundamental rights."

The rule of law is an implied limitation on the authority of any institution in a constitutional democracy.[591]

331 Interim orders of courts are an integral element of judicial review. Interim directions issued on the basis of the *prima facie* findings in a case are

[589] Ibid, at pages 128-129
[590] (2007) 2 SCC 1
[591] K.T. Plantation (P) Ltd. v. State of Karnataka, (2011) 9 SCC 1

temporary arrangements till the matter is finally decided. Interim orders ensure that the cause which is being agitated does not become infructuous before the final hearing.[592] The power of judicial review is not only about the writs issued by superior courts or the striking down of governmental action. Entrustment of judicial review is accompanied by a duty to ensure that judicial orders are complied with. Unless orders are enforced, citizens will lose faith in the efficacy of judicial review and in the legal system.

It is in the background of the above constitutional position that this Court must deal with the contention that the interim orders passed by this Court, during the adjudication of the present dispute were not observed. This Court has consistently insisted, through its interim orders, on a restraint on the mandatory use of Aadhaar. It has been submitted that the interim orders have been violated and several contempt petitions are pending[593] before this Court.

332 Prior to the enactment of the Aadhaar Act, the scheme was challenged before this Court. By its interim order dated 23 September 2013[594], a two judge Bench directed:

> "All the matters require to be heard finally. List all matters for final hearing after the Constitution Bench is over.
> **In the meanwhile, no person should suffer for not getting the Aadhaar card in spite of the fact that some authority had issued a circular making it mandatory and when any person applies to get the Aadhaar Card voluntarily, it may be checked whether that person is entitled for it**

[592]State of Assam v. Barak Upatyaka DU Karmachari Sanstha, (2009) 5 SCC 694
[593]Contempt Petition (Civil) No. 144/2014 in WP (C) No. 494/2012; Contempt Petition (Civil) No. 674/2014 in WP (C) No. 829/2013; Contempt Petition (Civil) No 444/2016 in WP (C) No. 494/2012
[594]The interim order was in WP (Civil No. 494 of 2012)

> **under the law and it should not be given to any illegal immigrant.**" (sic)

This was followed by an order dated 26 November 2013 where the earlier order was continued:

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

While considering another petition, **Unique Identification Authority of India** v **Central Bureau of Investigation**[595], this Court directed in an interim order dated 24 March 2014:

> "In the meanwhile, the present petitioner is restrained from transferring any biometric information of any person who has been allotted the Aadhaar number to any other agency without his consent in writing… **More so, no person shall be deprived of any service for want of Aadhaar number in case he/she is otherwise eligible/entitled. All the authorities are directed to modify their forms/circulars/likes so as to not compulsorily require the Aadhaar number in order to meet the requirement of the interim order passed by this Court forthwith**… Tag and list the matter with main matter i.e. WP(C) No.494/2012."

On 16 March 2015, while considering WP (Civil) 494 of 2012, this Court noted a violation of its earlier order dated 23 September 2013 and directed thus:

> "The matters require considerable time for hearing… **In the meanwhile, it is brought to our notice that in certain quarters, Aadhaar identification is being insisted upon by the various authorities. We do not propose to go into the specific instances. Since Union of India is represented by learned Solicitor General and all the States are represented through their respective counsel, we expect**

[595] SLP (Crl.) No. 2524/2015

> **that both the Union of India and States and all their functionaries should adhere to the Order passed by this Court on 23rd September, 2013**."

By an order dated 11 August 2015, a three judge Bench referred the issue as to whether privacy is a fundamental right to a bench of a larger strength of judges. The following interim directions were issued:

> "Having considered the matter, we are of the view that the balance of interest would be best served, till the matter is finally decided by a larger Bench if the Union of India or the UIDAI proceed in the following manner:-
> 1. The Union of India shall give wide publicity in the electronic and print media including radio and television networks that it is not mandatory for a citizen to obtain an Aadhaar card;
> 2. The production of an Aadhaar card will not be condition for obtaining any benefits otherwise due to a citizen;
> 3. The Unique Identification Number or the Aadhaar card will not be used by the respondents for any purpose other than the PDS Scheme and in particular for the purpose of distribution of foodgrains, etc. and cooking fuel, such as kerosene. The Aadhaar card may also be used for the purpose of the LPG Distribution Scheme;
> 4. The information about an individual obtained by the Unique Identification Authority of India while issuing an Aadhaar card shall not be used for any other purpose, save as above, except as may be directed by a Court for the purpose of criminal investigation."

On 15 October 2015, a Constitution Bench of this Court partially modified the order dated 11 August 2015, thus:

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

> 4. We impress upon the Union of India that it shall strictly follow all the earlier orders passed by this Court commencing from 23.09.2013.
> 5. We will also make it clear that the Aadhaar card Scheme is purely voluntary and it cannot be made mandatory till the matter is finally decided by this Court one way or the other."

After the Aadhaar Act was enacted there was a challenge in **All Bengal Minority Students Council** v **Union of India**[596], to a letter written to the Chief Secretaries/Administrators of all State Governments/Union territory Administrations by the Under Secretary to the Government of India, by which the requirement of the submission of Aadhaar for claiming benefits under a scheme was made mandatory. By an order dated 14 September 2016, a two judge Bench directed as follows:

> "…we stay the operation and implementation of letters dated 14.07.2006 (i.e. Annexure P-5, P-6 and P-7) for Pre-Matric Scholarship Scheme, Post-Matric Scholarship Scheme and Merit-cum-Means Scholarship Scheme to the extent they have made submission of Aadhaar mandatory and direct the Ministry of Electronics and Information Technology, Government of India i.e. Respondent No.2 to remove Aadhaar number as a mandatory condition for student Registration form at the National Scholarship Portal of Ministry of Electronics and Information Technology, Government of India at the website http://scholarships.gov.in/newStudentRegFrm and stay the implementation of clause (c) of the 'Important Instructions' of the advertisement dated 20.08.2016 for the Pre-Matric Scholarship Scheme, Post-Matric Scholarship Scheme and Merit-cum-Means Scholarship Scheme, during the pendency of this writ petition."

It has been submitted that the notifications and circulars, which make the application of Aadhaar mandatory, are contrary to the interim orders passed by this Court. It has been contended that the Respondents have flouted the

[596] WP (Civil) No. 686/2016

most elementary norms of good governance and have disrespected judicial orders. This contention requires serious consideration.

333 The legislature cannot simply declare that the judgment of a court is invalid or that it stands nullified. In **Kalpana Mehta**, a Constitution Bench of this Court held:

> "255…If the legislature were permitted to do so, it would travel beyond the boundaries of constitutional entrustment. While the separation of powers prevents the legislature from issuing a mere declaration that a judgment is erroneous or invalid, the law-making body is entitled to enact a law which remedies the defects which have been pointed out by the court. Enactment of a law which takes away the basis of the judgment (as opposed to merely invalidating it) is permissible and does not constitute a violation of the separation doctrine. That indeed is the basis on which validating legislation is permitted."[597]

Where a final judgment or order of this Court is sought to be undone by an Act of Parliament, it is imperative that the basis of the Court's judgment or order is removed. It has been held by this Court in **Bhubaneshwar Singh** v **Union of India**[598]:

> "11. From time to time controversy has arisen as to whether the effect of judicial pronouncements of the High Court or the Supreme Court can be wiped out by amending the legislation with retrospective effect. Many such Amending Acts are called Validating Acts, validating the action taken under the particular enactments by removing the defect in the statute retrospectively because of which the statute or the part of it had been declared ultra vires. Such exercise has been held by this Court as not to amount to encroachment on the judicial power of the courts. **The exercise of rendering ineffective the judgments or orders of competent courts by changing the very basis by legislation is a well-known device of validating legislation.** This Court has repeatedly pointed out

[597] Ibid, at page 126
[598] (1994) 6 SCC 77

> that such validating legislation which removes the cause of the invalidity cannot be considered to be an encroachment on judicial power. **At the same time, any action in exercise of the power under any enactment which has been declared to be invalid by a court cannot be made valid by a Validating Act by merely saying so unless the defect which has been pointed out by the court is removed with retrospective effect. The validating legislation must remove the cause of invalidity. Till such defect or the lack of authority pointed out by the court under a statute is removed by the subsequent enactment with retrospective effect, the binding nature of the judgment of the court cannot be ignored.**"[599] (Emphasis supplied)

When the Aadhaar Act was notified on 25 March 2016, the interim directions issued by this court were in operation. Was it then open to government to launch upon a virtual spree of administrative notifications making Aadhaar a mandatory requirement of virtually every aspect of human existence from birth until death?

The position which the Union government has adopted before this court is simply this: interim directions were issued by this court when the Aadhaar project was governed by executive instructions. Once a law was enacted by Parliament, a statutory authorisation was brought into existence to enable government to issue administrative instructions. Hence, compliance with the interim orders stands obviated upon the enactment of the law.

334 This defence of government can be scrutinized at two levels – the first as a matter of statutory interpretation and the second, on a broader foundation which engages the judicial power of this court. As a matter of

[599] Ibid at pages 83-84

statutory interpretation, the Aadhaar Act did not, as it could not have, merely nullified the interim orders of this court. Section 59 has no provision which gives it overriding effect notwithstanding any judgment, decree or order of a court. The interim orders do not stand superseded. Apart from approaching the issue purely as a matter of statutory interpretation, there are broader concerns which arise from the manner in which the authorities proceeded, oblivious to the interim directions. Interim directions were issued by this court in a situation where a constitutional challenge was addressed in a batch of petitions on the ground that the Aadhaar project was offensive to fundamental rights, including the right to privacy. So significant was the nature of the challenge that it was referred initially to a Constitution Bench and thereafter, to a bench of nine-judges of this Court for resolving the question as to whether privacy is a protected fundamental right. The collection and storage of biometric data and its use for the purpose of authentication is the subject of a constitutional challenge. Noting the nature of the challenge and after considering the serious issues which have arisen in the case, successive benches of this Court issued a series of interim directions. The purport of those directions is that Aadhaar could not be made mandatory except for specified schemes which were listed by the court. Moreover, in the context of the serious grievance of financial exclusion, the court directed that no individual should be excluded from the receipt of welfare entitlements, such as food-grains, for want of an Aadhaar number. The constitutional challenge was not obviated merely on the enactment of the Aadhaar Act. The law gave a

statutory character to a project which since 2009 was possessed of an administrative or executive nature. The constitutional challenge to some of the basic features underlying the collection of biometric data still remained to be addressed by the court. The proceedings before this Court are testimony to the fact that the issue of constitutionality was indeed live. That being the position, the issuance of a spate of administrative notifications is in defiance of the interim orders passed by this Court. Judicial orders, be they interim or final, cannot simply be wished away. If governments or citizens were allowed to ignore judicially enforceable directions, that would negate the basis of the rule of law. Both propriety and constitutional duty required Union government to move this Court after the enactment of the Aadhaar Act for variation of the interim orders. Such an application would have required this Court to weigh on the one hand the subsequent development of the law being passed (something which would be relied upon by government) with the constitutional concerns over the entire biometric project. It is not as if that the mere enactment of the law put an end to the constitutional challenge. The existence of law (post 2016) is only one aspect to be considered in deciding the interim arrangement which would hold the field when the constitutional challenge was pending adjudication before this Court. Institutions of governance are bound by a sense of constitutional morality which requires them to abide by judicial orders. What seems to emerge from the course of action which has been followed in the present case by government is a perception that judicial directions can be ignored on a supposed construction of the statute. Besides

the fact that this construction is erroneous in law, it is above all, the fundamental duty of this Court to ensure that its orders are not treated with disdain. If we were not to enforce a punctilious compliance with our own directions by government, that would ring a death – knell of the institutional position of the Supreme Court. If governments were free to ignore judicial directions at will, could a different yardstick be applied to citizens? The obligation to comply with judicial orders is universal to our polity and admits of no exception. Confronted with a brazen disregard of our interim orders, I believe that we have no course open except to stand firm.

335 The power of judicial review conferred on an independent judiciary requires that other organs of the State respect the authority of Courts. This Court in **P Sambamurthy** v **State of Andhra Pradesh**[600], while highlighting the importance of judicial review in the rule of law regime, held thus:

> "4… it is a basic principle of the rule of law that the exercise of power by the executive or any other authority must not only be conditioned by the Constitution but must also be in accordance with law and the power of judicial review is conferred by the Constitution with view to ensuring that the law is observed and there is compliance with the requirement of law on the part of the executive and other authorities. It is through the power of judicial review conferred on an independent institutional authority such as the High Court that the rule of law is maintained and every organ of the State is kept within the limits- of the law. Now **if the exercise of the power of judicial review can be set at naught by the State Government by overriding the decision given against it, it would sound, the death-knell of the rule of law. The rule of law would cease to have any meaning, because then it would be open to the State Government to defy the law and yet get away with it.**"[601] (Emphasis supplied)

[600] (1987) 1 SCC 362
[601] Ibid, at page 369

336 A Bench of two judges in **Re: Arundhati Roy**[602] held that for the courts to protect the rule of law, it is necessary that the dignity and authority of the courts have to be respected and protected. It was held:

> "'Rule of Law' is the basic rule of governance of any civilised democratic policy. Our Constitutional scheme is based upon the concept of Rule of Law which we have adopted and given to ourselves. Everyone, whether individually or collectively is unquestionably under the supremacy of law. Whoever the person may be, however high he or she is, no-one is above the law notwithstanding how powerful and how rich he or she may be. **For achieving the establishment of the rule of law, the Constitution has assigned the special task to the judiciary in the country. It is only through the courts that the rule of law unfolds its contents and establishes its concept. For the judiciary to perform its duties and functions effectively and true to the spirit with which it is sacredly entrusted, the dignity and authority of the courts have to be respected and protected at all costs.**"[603] (Emphasis supplied)

The accountability of power, as a component of the rule of law, requires that the power vested in any organ of the State, and its agents, can only be used for promotion of constitutional values and vision.[604] Governmental authority may only be exercised in accordance with written laws which are adopted though an established procedure. No action of the legislature or the executive can undermine the authority of the courts, except according to established principles. Disrespect of court orders results in impairment of the dignity of the courts.

[602] (2002) 3 SCC 343
[603] Ibid, at page 346
[604] Nandini Sundar v State of Chhattisgarh, (2011) 7 SCC 547

337 Constitutional morality requires a government not to act in a manner which would become violative of the rule of law.[605] Constitutional morality requires that the orders of this Court be complied with, faithfully. This Court is the ultimate custodian of the Constitution. The limits set by the Constitution are enforced by this Court. Constitutional morality requires that the faith of the citizens in the constitutional courts of the country be maintained. The importance of the existence of courts in the eyes of citizens has been highlighted in Harper Lee's classic "To Kill a Mockingbird":

> "But **there is one way in this country in which all men are created equal**—there is one human institution that makes a pauper the equal of a Rockefeller, the stupid man the equal of an Einstein, and the ignorant man the equal of any college president. **That institution, gentlemen, is a court.** It can be the Supreme Court of the United States or the humblest J.P. court in the land, or this honorable court which you serve. Our courts have their faults, as does any human institution, but in this country our courts are the great levelers, and in our courts all men are created equal." (Emphasis supplied)

Many citizens, although aggrieved, are not in a condition to reach the highest Court. The poorest and socially neglected lack resources and awareness to reach this Court. Their grievances remain unaddressed. Such individuals suffer injury each day without remedy. Disobedience of the interim orders of this Court and its institutional authority, in the present case, has made a societal impact. It has also resulted in denial of subsidies and other benefits essential to the existence of a common citizen. Constitutional morality therefore needs to be enforced as a valid response to these arbitrary acts. Non-compliance of the interim orders of this Court is contrary to constitutional

[605] Manoj Narula v Union of India, (2014) 9 SCC 1

morality. Constitutional morality, as an essential component of the rule of law, must neutralise the excesses of power by the executive. The brazen manner in which notifications have been issued making Aadhaar mandatory, despite the interim order of this Court is a matter of serious concern. Deference to the institutional authority of the Supreme Court is integral to the values which the Constitution adopts. The postulate of a limited government is enforced by the role of the Supreme Court in protecting the liberties of citizens and holding government accountable for its transgressions. The authority of this Court is crucial to maintaining the fine balances of power on which democracy thrives and survives. The orders of the Court are not recommendatory – they are binding directions of a constitutional adjudicator. Dilution of the institutional prestige of this Court can only be at the cost of endangering the freedom of over a billion citizens which judicial review seeks to safeguard.

338 Courts – as it is often said- have neither the power of the purse nor the sword. Our authority lies in constitutional legitimacy as much as in public confidence. Combined together they impart moral and institutional authority to the Court. That sense of legitimacy and duty have required me to assert once again the norms of a written Constitution and the rule of law. This judgment has taken a much wider postulation. Having held the Aadhaar Act prior to its passage not to be a Money Bill, I have delved into the merits of the constitutional challenge for two reasons:

i. Merits have been argued in considerable detail both by petitioners and the Union of India; and

ii. As a logical consequence of the view that the Aadhaar legislation is not a Money Bill, it would be open to the government to reintroduce fresh legislation. The principles governing a law regulating the right to data protection and informational privacy have hence been delineated.

L Conclusion

339 The present dispute has required this Court to analyze the provisions of the Aadhaar Act and Regulations, along with the framework as it existed prior to the enactment of the Act, through the prism of the Constitution and the precedents of this Court. My conclusions are outlined below:

(1) In order to deal with the challenge that the Aadhaar Act should not have been passed as a Money Bill, this Court was required to adjudicate whether the decision of the Speaker of the Lok Sabha to certify a Bill as a Money Bill, can be subject to judicial review. The judgment has analyzed the scope of the finality attributed to the Speaker's decision, by looking at the history of Article 110(3) of the Constitution, by comparing it with the comparative constitutional practices which accord finality to the Speaker's decision, by analyzing other constitutional provisions which use the phrase

"shall be final", and by examining the protection granted to parliamentary proceedings under Article 122. This judgment holds that:

(a) The phrase "shall be final" used under Article 110(3) aims at avoiding any controversy on the issue as to whether a Bill is a Money Bill, with respect to the Rajya Sabha and before the President. The language used in Article 110(3) does not exclude judicial review of the Speaker's decision. This also applies to Article 199(3).

(b) The immunity from judicial review provided to parliamentary proceedings under Article 122 is limited to instances involving "irregularity of procedure". The decisions of this Court in **Special Reference, Ramdas Athawale** and **Raja Ram Pal** hold that the validity of proceedings in Parliament or a State Legislature can be subject to judicial review when there is a substantive illegality or a constitutional violation. These judgments make it clear that the decision of the Speaker is subject to judicial review, if it suffers from illegality or from a violation of constitutional provisions.

(c) Article 255 has no relation with the decision of the Speaker on whether a Bill is a Money Bill. The three Judge Bench decision in **Mohd Saeed Siddiqui** erroneously interpreted the judgment in **Mangalore Beedi** to apply Articles 212 (or Article 122) and 255 to refrain from questioning the conduct of the Speaker (under Article 199 or 110). The two judge

Bench decision in **Yogendra Kumar** followed **Mohd Saeed Siddiqui**. The correct position of law is that the decision of the Speaker under Articles 110(3) and 199(3) is not immune from judicial review. The decisions in **Mohd Saeed Siddiqui** and **Yogendra Kumar** are accordingly overruled.

(d) The existence of and the role of the Rajya Sabha, as an institution of federal bicameralism in the Indian Parliament, constitutes a part of the basic structure of the Constitution. The decision of the Speaker of the Lok Sabha to certify a Bill as a Money Bill has a direct impact on the role of the Rajya Sabha, since the latter has a limited role in the passing of a Money Bill. A decision of the Speaker of the Lok Sabha to declare an ordinary Bill to be a Money Bill limits the role of the Rajya Sabha. The power of the Speaker cannot be exercised arbitrarily in violation of constitutional norms and values, as it damages the essence of federal bicameralism, which is a part of the basic structure of the Constitution. Judicial review of the Speaker's decision, on whether a Bill is a Money Bill, is therefore necessary to protect the basic structure of the Constitution.

(2) To be certified a Money Bill, a Bill must contain "only provisions" dealing with every or any one of the matters set out in sub-clauses (a) to (g) of Article 110(1). A Bill, which has both provisions which fall within sub-clauses (a) to (g) of Article 110(1) and provisions which fall outside their

scope, will not qualify to be a Money Bill. Thus, when a Bill which has been passed as a Money Bill has certain provisions which fall beyond the scope of sub-clauses (a) to (g) of Article 110(1), these provisions cannot be severed. If the bill was not a Money Bill, the role of the Rajya Sabha in its legislative passage could not have been denuded. The debasement of a constitutional institution cannot be countenanced by the Court. Democracy survives when constitutional institutions are vibrant.

(3) The Aadhaar Act creates a statutory framework for obtaining a unique identity number, which is capable of being used for "any" purpose, among which availing benefits, subsidies and services, for which expenses are incurred from the Consolidated Fund of India, is just one purpose provided under Section 7. Clause (e) of Article 110(1) requires that a Money Bill must deal with the declaring of any expenditure to be expenditure charged on the Consolidated Fund of India (or increasing the amount of the expenditure). Section 7 fails to fulfil this requirement. Section 7 does not declare the expenditure incurred to be a charge on the Consolidated Fund. It only provides that in the case of such services, benefits or subsidies, Aadhaar can be made mandatory to avail of them. Moreover, provisions other than Section 7 of the Act deal with several aspects relating to the Aadhaar numbers: enrolment on the basis of demographic and biometric information, generation of Aadhaar numbers, obtaining the consent of individuals before collecting their individual information,

creation of a statutory authority to implement and supervise the process, protection of information collected during the process, disclosure of information in certain circumstances, creation of offences and penalties for disclosure or loss of information, and the use of the Aadhaar number for "any purpose". All these provisions of the Aadhaar Act do not lie within the scope of sub-clauses (a) to (g) of Article 110(1). Hence, in the alternate, even if it is held that Section 7 bears a nexus to the expenditure incurred from the Consolidated Fund of India, the other provisions of the Act fail to fall within the domain of Article 110(1). Thus, the Aadhaar Act is declared unconstitutional for failing to meet the necessary requirements to have been certified as a Money Bill under Article 110(1).

(4) The argument that the Aadhaar Act is in pith and substance a Money Bill, with its main objective being the delivery of subsidies, benefits and services flowing out of the Consolidated Fund of India and that the other provisions are ancillary to the main purpose of the Act also holds no ground, since the doctrine of pith and substance is used to examine whether the legislature has the competence to enact a law with regard to any of the three Lists in the Seventh Schedule of the Constitution. The doctrine cannot be invoked to declare whether a Bill satisfies the requirements set out in Article 110 of the Constitution to be certified a Money Bill. The argument of the Union of India misses the point that a Bill

can be certified as a Money Bill "**only**" if it deals with all or any of the matters contained in clauses (a) to (g) of Article 110(1).

(5) Having held that the Aadhaar Act is unconstitutional for having been passed as a Money Bill this judgment has also analysed the merits of the other constitutional challenges to the legislation as well as to the framework of the project before the law was enacted.

(6) The architecture of the Aadhaar Act seeks to create a unique identity for residents on the basis of their demographic and biometric information. The Act sets up a process of identification by which the unique identity assigned to each individual is verified with the demographic and biometric information pertaining to that individual which is stored in a centralised repository of data. Identification of beneficiaries is integral and essential to the fulfilment of social welfare schemes and programmes, which are a part of the State's attempts to ensure that its citizens have access to basic human facilities. This judgment accepts the contention of the Union of India that there is a legitimate state aim in maintaining a system of identification to ensure that the welfare benefits provided by the State reach the beneficiaries who are entitled, without diversion.

(7) The Aadhaar programme involves application of biometric technology, which uses an individual's biometric data as the basis of authentication or identification and is therefore intimately connected to the individual. While

citizens have privacy interests in personal or private information collected about them, the unique nature of biometric data distinguishes it from other personal data, compounding concerns regarding privacy protections safeguarding biometric information. Once a biometric system is compromised, it is compromised forever. Therefore, it is imperative that concerns about protecting privacy must be addressed while developing a biometric system. Adequate norms must be laid down for each step from the collection to retention of biometric data. At the time of collection, individuals must be informed about the collection procedure, the intended purpose of the collection, the reason why the particular data set is requested and who will have access to their data. Additionally, the retention period must be justified and individuals must be given the right to access, correct and delete their data at any point in time, a procedure familiar to an opt-out option.

(8) Prior to the enactment of the Aadhaar Act, no mandatory obligation was imposed upon the Registrars or the enrolling agencies, to obtain informed consent from residents before recording their biometric data, to inform them how the biometric data would be stored and used and about the existence of adequate safeguards to secure the data. Moreover, prior to the enactment of the Act, while UIDAI had itself contemplated that an identity theft could occur at the time of enrollment for Aadhaar cards, it

had no solution to the possible harms which could result after the identity theft of a person.

(9) The Regulations framed subsequently under the Aadhaar Act also do not provide a robust mechanism on how informed consent is to be obtained from residents before collecting their biometric data. The Aadhaar Act and Regulations are bereft of the procedure through which an individual can access information related to his or her authentication record. The Aadhaar Act clearly has no defined options that should be made available to the Aadhaar number holders in case they do not wish to submit identity information during authentication, nor do the regulations specify the procedure to be followed in case the Aadhaar number holder does not provide consent for authentication.

(10) Sections 29(1) and (2) of the Act create a distinction between two classes of information (core biometric information and identity information), which are integral to individual identity and require equal protection. Section 29(4) suffers from overbreadth as it gives wide discretionary power to UIDAI to publish, display or post core biometric information of an individual for purposes specified by the regulations.

(11) Sections 2(g), (j), (k) and (t) suffer from overbreadth, as these can lead to an invasive collection of biological attributes. These provisions give

discretionary power to UIDAI to define the scope of biometric and demographic information and empower it to expand on the nature of information already collected at the time of enrollment, to the extent of also collecting any *"such other biological attributes*" that it may deem fit.

(12) There is no clarity on how an individual is supposed to update his/her biometric information, in case the biometric information mismatches with the data stored in CIDR. The proviso to Section 28(5) of the Aadhaar Act, which disallows an individual access to the biometric information that forms the core of his or her unique ID, is violative of a fundamental principle that ownership of an individual's data must at all times vest with the individual. UIDAI is also provided wide powers in relation to removing the biometric locking of residents. With this analysis of the measures taken by the Government of India prior to the enactment of the Aadhaar Act as well as a detailed analysis of the provisions under the Aadhaar Act, 2016 and supporting Regulations made under it, this judgment concludes that the Aadhaar programme violates essential norms pertaining to informational privacy, self-determination and data protection.

(13) The State is under a constitutional obligation to safeguard the dignity of its citizens. Biometric technology which is the core of the Aadhaar programme is probabilistic in nature, leading to authentication failures. These authentication failures have led to the denial of rights and legal

entitlements. The Aadhaar project has failed to account for and remedy the flaws in its framework and design which has led to serious instances of exclusion of eligible beneficiaries as demonstrated by the official figures from Government records including the Economic Survey of India 2016-17 and research studies. Dignity and the rights of individuals cannot be made to depend on algorithms or probabilities. Constitutional guarantees cannot be subject to the vicissitudes of technology. Denial of benefits arising out of any social security scheme which promotes socio-economic rights of citizens is violative of human dignity and impermissible under our constitutional scheme.

(14) 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:

(a) 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 recognized 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 meta-data 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.

(b) 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.

(c) 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.

(d) Before the enactment of the Aadhaar Act, MOUs signed between UIDAI and Registrars were not contracts within the purview of Article 299 of the Constitution, and therefore, do not cover the acts done by the private entities engaged by the Registrars for enrolment. Since there is no privity of contract between UIDAI and the Enrolling agencies, the activities of the private parties engaged in the process of enrolment before the enactment of the Aadhaar Act have no statutory or legal backing.

(e) Under the Aadhaar architecture, UIDAI is the sole authority which carries out all administrative, adjudicatory, investigative, and monitoring functions of the project. While the Act confers these functions on UIDAI, it does not place any institutional accountability upon UIDAI to protect the database of citizens' personal information. UIDAI also takes no institutional responsibility for verifying whether the data entered and

stored in the CIDR is correct and authentic. The task has been delegated to the enrolment agency or the Registrar. Verification of data being entered in the CIDR is a highly sensitive task for which the UIDAI ought to have taken responsibility. The Aadhaar Act is also silent on the liability of UIDAI and its personnel in case of their non-compliance of the provisions of the Act or the regulations.

(f) Section 47 of the Act violates citizens' right to seek remedies. Under Section 47(1), a court can take cognizance of an offence punishable under the Act only on a complaint made by UIDAI or any officer or person authorised by it. Section 47 is arbitrary as it fails to provide a mechanism to individuals to seek efficacious remedies for violation of their right to privacy. Further, Section 23(2)(s) of the Act requires UIDAI to establish a grievance redressal mechanism. Making the authority which is administering a project, also responsible for providing a grievance redressal mechanism for grievances arising from the project severely compromises the independence of the grievance redressal body.

(g) While the Act creates a regime of criminal offences and penalties, the absence of an independent regulatory framework renders the Act largely ineffective in dealing with data violations. The architecture of Aadhaar ought to have, but has failed to embody within the law the establishment of an independent monitoring authority (with a hierarchy

of regulators), along with the broad principles for data protection. This compromise in the independence of the grievance redressal body impacts upon the possibility and quality of justice being delivered to citizens. In the absence of an independent regulatory and monitoring framework which provides robust safeguards for data protection, the Aadhaar Act cannot pass muster against a challenge on the ground of reasonableness under Article 14.

(h) No substantive provisions, such as those providing data minimization, have been laid down as guiding principles for the oversight mechanism provided under Section 33(2), which permits disclosure of identity information and authentication records in the interest of national security.

(i) 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.

(j) 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.

(k) Section 7 suffers from overbreadth since the broad definitions of the expressions ‘services and ‘benefits’ enable the government to regulate almost every facet of its engagement with citizens under the Aadhaar platform. If the requirement of Aadhaar is made mandatory for every benefit or service which the government provides, it is impossible to live in contemporary India without Aadhaar. The inclusion of services and benefits in Section 7 is a pre-cursor to the kind of function creep which is inconsistent with the right to informational self-determination. Section 7 is therefore arbitrary and violative of Article 14 in relation to the inclusion of services and benefits as defined.

(l) The legitimate aim of the State can be fulfilled by adopting less intrusive measures as opposed to the mandatory enforcement of the Aadhaar scheme as the sole repository of identification. The State has failed to demonstrate that a less intrusive measure other than biometric

authentication would not subserve its purposes. That the state has been able to insist on an adherence to the Aadhaar scheme without exception is a result of the overbreadth of Section 7.

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

(n) One right cannot be taken away at the behest of the other. The State has failed to satisfy this Court that the targeted delivery of subsidies which animate the right to life entails a necessary sacrifice of the right to individual autonomy, data protection and dignity when both these rights are protected by the Constitution.

(15) Section 59 of the Aadhaar Act seeks to retrospectively validate the actions of the Central Government done prior to the Aadhaar Act pursuant to Notifications dated 28 January 2009. and 12 September 2015. Section 59 does not validate actions of the state governments or of private entities. Moreover, the notification of 2009 did not authorise the collection of biometric data. Consequently, the validation of actions taken under the 2009 notification by Section 59 does not save the collection of biometric data prior to the enforcement of the Act. While Parliament

possesses the competence to enact a validating law, it must cure the cause of infirmity or invalidity. Section 59 fails to cure the cause of invalidity prior to the enactment of the Aadhaar Act. The absence of a legislative framework for the Aadhaar project between 2009 and 2016 left the biometric data of millions of Indian citizens bereft of the kind of protection which must be provided to comprehensively protect and enforce the right to privacy. Section 59 therefore fails to meet the test of a validating law since the complete absence of a regulatory framework and safeguards cannot be cured merely by validating what was done under the notifications of 2009 and 2016.

(16) The decision in **Puttaswamy** recognised that revenue constitutes a legitimate state aim in the three-pronged test of proportionality. However, the existence of a legitimate aim is insufficient to uphold the validity of the law, which must also meet the other parameters of proportionality spelt out in **Puttaswamy.**

(17) The seeding of Aadhaar with PAN cards depends on the constitutional validity of the Aadhaar legislation itself. Section 139AA of the Income Tax Act 1962 is based on the premise that the Aadhaar Act itself is a valid legislation. Since the Aadhaar Act itself is now held to be unconstitutional for having been enacted as a Money Bill and on the touchstone of proportionality, the seeding of Aadhaar to PAN under Article 139AA does not stand independently.

(18) The 2017 amendments to the PMLA Rules fail to satisfy the test of proportionality. The imposition of a uniform requirement of linking Aadhaar numbers with all account based relationships proceeds on the presumption that all existing account holders as well as every individual who seeks to open an account in future is a potential money-launderer. No distinction has been made in the degree of imposition based on the client, the nature of the business relationship, the nature and value of the transactions or the actual possibility of terrorism and money- laundering. The rules also fail to make a distinction between opening an account and operating an account. Moreover, the consequences of the failure to submit an Aadhaar number are draconian. In their present form, the rules are clearly disproportionate and excessive. We clarify that this holding would not preclude the Union Government in the exercise of its rule making power and the Reserve Bank of India as the regulator to re-design the requirements in a manner that would ensure due fulfillment of the object of preventing money-laundering, subject to compliance with the principles of proportionality as outlined in this judgment.

(19) Mobile phones have become a ubiquitous feature of the lives of people and the linking of Aadhaar numbers with SIM cards and the requirement of e-KYC authentication of mobile subscribers must necessarily be viewed in this light. Applying the proportionality test, the legitimate aim of subscriber verification, has to be balanced against the countervailing requirements of

preserving the integrity of biometric data and the privacy of mobile phone subscribers. Mobile phones are a storehouse of personal data and reflect upon individual preferences, lifestyle and choices. The conflation of biometric information with SIM cards poses grave threats to individual privacy, liberty and autonomy. Having due regard to the test of proportionality which has been propounded in **Puttaswamy** and as elaborated in this judgment, the decision to link Aadhaar numbers with mobile SIM cards is neither valid nor constitutional. The mere existence of a legitimate state aim will not justify the disproportionate means which have been adopted in the present case. The biometric information and Aadhaar details collected by Telecom Service Providers shall be deleted forthwith and no use of the said information or details shall be made by TSPs or any agency or person or their behalf.

(20) Defiance of judicial orders (both interim and final) be it by the government or by citizens negates the basis of the rule of law. Both propriety and constitutional duty required the Union government to move this Court after the enactment of the Aadhaar Act for variation of this Court's interim orders. Institutions of governance are bound by a sense of constitutional morality which requires them to abide by judicial orders.

(21) Identity is necessarily a plural concept. The Constitution also recognizes a multitude of identities through the plethora of rights that it safeguards.

The technology deployed in the Aadhaar scheme reduces different constitutional identities into a single identity of a 12-digit number and infringes the right of an individual to identify herself/himself through a chosen means. Aadhaar is about identification and is an instrument which facilitates a proof of identity. It must not be allowed to obliterate constitutional identity.

(22) The entire Aadhaar programme, since 2009, suffers from constitutional infirmities and violations of fundamental rights. The enactment of the Aadhaar Act does not save the Aadhaar project. The Aadhaar Act, the Rules and Regulations framed under it, and the framework prior to the enactment of the Act are unconstitutional.

(23) To enable the government to initiate steps for ensuring conformity with this judgment, it is directed under Article 142 that the existing data which has been collected shall not be destroyed for a period of one year. During this period, the data shall not be used for any purpose whatsoever. At the end of one year, if no fresh legislation has been enacted by the Union government in conformity with the principles which have been enunciated in this judgment, the data shall be destroyed.

Creating strong privacy protection laws and instilling safeguards may address or at the very least assuage some of the concerns associated with the Aadhaar scheme which severely impairs informational self-determination,

individual privacy, dignity and autonomy. In order to uphold the democratic values of the Constitution, the government needs to address the concerns highlighted in this judgment which would provide a strong foundation for digital initiatives, which are imminent in today's digital age. However, in its current form, the Aadhaar framework does not sufficiently assuage the concerns that have arisen from the operation of the project which have been discussed in this judgment.

…….....J
[Dr Dhananjaya Y Chandrachud]

New Delhi;
September 26, 2018.